9

Privacy Measures to Combat Cyber Crime

Introduction

9.1 Vast amounts of personal information are increasingly being transmitted over the Internet and stored on digital devices. Contributors to the inquiry argued that this growing amount of digitised personal information places end users at a higher risk of identity theft and fraud, and argued that ensuring the privacy of end users' personal information is central to the prevention of cyber crime.[1]

9.2 The Office of the Victorian Privacy Commissioner (OVPC) submitted:

> The protection of information privacy, and reduction of e-security risks, are closely related concepts. Cyber crimes necessarily involve an invasion of an individual's privacy, through access or fraudulent use of personal information.[2]

9.3 This section briefly describes the legislative framework for privacy protection in Australia, and examines five key areas to further protect the personal information of Australian end users:

- issues relating to the *Privacy Act 1988* (Cth)(the *Privacy Act*);
- consistency between Commonwealth, State and Territory privacy regulation;
- industry codes of practice;

---

1 See for example: Australian Merchant Payments Forum, *Submission 17*, p.1; Internet Industry Association, *Submission 54*, p.4; Internet Society of Australia, *Submission 45*, p.5.

2 OVPC, *Submission 33*, p.2.

- international regulation and cooperation; and
- privacy audits.

Overview of Australian privacy protection legislation

9.4 The *Privacy Act* regulates the protection and use of personal information, including financial details and identity information. This is primarily achieved through two sets of privacy provisions: the Information Privacy Principles, which regulate Australian and Australian Capital Territory Government 'agencies'; and the National Privacy Principles, which regulate all private sector 'organisations' with an annual turnover of over $3 million. The *Privacy Act* establishes the Office of the Privacy Commissioner (OPC), an independent statutory body, to promote and protect privacy in Australia.[3]

9.5 The *Privacy Act* permits organisations to develop and enforce their own privacy codes that, once approved by the OPC, replace the National Privacy Principles for those organisations bound by the code. Codes must have a body established to oversee the operation of the code, and to receive complaints.[4]

9.6 The OPC has further responsibilities under: the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), in regulating government data-matching programs; the *National Health Act 1953* (Cth), in regulating the handling of health information collected under the Medicare and Pharmaceutical Benefits Scheme; the *Crimes Act 1914* (Cth), in regulating information on past convictions; and the *Telecommunications Act 1997* (Cth).[5]

9.7 The OPC's role in relation to the *Telecommunications Act* is of particular relevance to cyber crime, as it deals with the use and disclosure of certain information by telecommunications service providers. These regulations apply to the contents of a communication being transmitted by a carriage service, and information incidental to the delivery of a carriage service, such as Internet Protocol addresses, unlisted telephone numbers or any

3 OPC, *Submission 3*, pp.3-7.

4 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.263-264.

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.267.

address.[6] It is unclear whether such information would be considered personal information under the *Privacy Act*.[7]

9.8 It should be noted that the privacy provisions of the *Telecommunications Act* do not extend to information that may be collected by a telecommunications provider for purposes unrelated to the provision of a carriage service (such as a customer list purchased for marketing purposes). In such cases, the *Privacy Act* still plays a central role in protecting information held by telecommunications providers.[8] The Committee did not receive evidence on the adequacy of the privacy provisions of the *Telecommunications Act*, however the issue is discussed extensively in Chapter 71 of the ALRC's review.[9]

9.9 At the State and Territory level, most jurisdictions have additional legislation to regulate their respective public sector organisations, and to establish independent regulators. The exceptions are South Australia and Western Australia, who maintain administrative schemes to protect privacy, but do not currently have specific legislation or an independent regulator.[10]

9.10 In May 2008 the Australian Law Reform Commission (ALRC) completed a review of the *Privacy Act*. The ALRC's report, *For Your Information: Australian Privacy Law and Practice*, made 295 recommendations on a broad range of topics relating to the *Privacy Act* and the privacy legislative framework more broadly, including issues relating to the protection of privacy online.[11]

9.11 The Government is responding to the review in two stages. The first stage dealt with 197 of the recommendations and was released on 14 October 2009. The Government proposes to release draft legislation implementing the first stage response during 2010, and to consider the remaining 88 recommendations once the first stage of reforms has been progressed.[12]

---

6 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.2381-2382.

7 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.2382.

8 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.2382.

9 See: ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.2377-2412.

10 OVPC, *Submission 33*, p.3.

11 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.110-129.

12 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

The Privacy Act 1988

9.12 Submitters to the inquiry endorsed a number of the ALRC's recommendations as measures that would assist in combating cyber crime. These are:

- the removal of certain exemptions that currently apply to the *Privacy Act*;
- mandated reporting of data breaches experienced by organisations; and
- measures to prevent the over collection of personal information.[13]

9.13 The OVPC noted two significant exemptions in the regulation of privacy in the private sector. First, private sector employee records are specifically excluded from the *Privacy Act*.[14] The OVPC argue that employee records often contain detailed personal information which, without mandated protection, may be vulnerable to being compromised.[15] Second, 'small businesses' with an annual turnover of less than $3 million are exempt from the *Privacy Act*. The OVPC note that these businesses may obtain vast amounts of personal information in the course of their activities, but are under no obligation to take precautions to protect this information.[16] The ALRC also cited small ISPs as examples of organisations that handle large amounts of personal information but are currently exempt,[17] (although small ISPs do have limited privacy obligations under the *Telecommunications Act*).

9.14 The ALRC 's 2008 review acknowledged both exemptions as limitations on privacy protection, and concluded that the exemptions were unjustified. The ALRC recommended that the exemptions be removed from the *Privacy Act*.[18] The Government is considering these recommendations in the second stage of its response to the ALRC's review.[19] The OVPC argued that the removal of the exemptions would assist in protecting from cyber crime:

13 OVPC, *Submission 33*, pp.4-8; OPC, *Submission 3*, p.8; Symantec Corporation, *Submission 32.1*, p.3; Australian Communications Consumer Action Network, *Submission 57*, p.72.

14 Employee records are protected by law in some States, such as Victoria.

15 OVPC, *Submission 33*, p.4.

16 OVPC, *Submission 33*, p.4.

17 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1356.

18 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1392-1398, 1355-1356.

19 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

> Enhancement and expansion of existing privacy laws, to close exemptions and to ensure more organisations are covered, will go a long way to reduce potential data loss or privacy breaches. This in turn will reduce the potential for identity fraud or theft to be committed.[20]

9.15 The reporting of data breaches, or lack thereof, was also raised as a privacy issue. Symantec submitted that large amounts of personal information retained by private businesses continue to be compromised by data breaches, and that such compromises lead to a high risk of identity crime and fraud.[21] Currently, companies are not required to report to a regulator, or to notify individuals, when personal information retained on their system has been compromised by a data breach.[22] Companies may voluntarily report such breaches to a privacy commissioner, or directly to individual victims (the OPC has developed a guide to this effect)[23], however witnesses argued that many organisations continue to have a strong incentive to protect their reputation by not reporting breaches.[24] Both the OPC and OVPC argued that notifying individuals that their details have been compromised may permit individuals to take actions to mitigate the resulting risk of identity theft and fraud.[25]

9.16 The ALRC's 2008 review recommended that the *Privacy Act* should be amended to require an agency or organisation to notify the OPC, and affected individuals, when certain personal information is reasonably believed to have been compromised.[26] The Government is considering this recommendation in the second stage of its response to the ALRC's review.[27]

---

20 OVPC, *Submission 33*, p.4.

21 Symantec Corporation, *Submission 32.1*, p.3.

22 Fujitsu Australia Ltd, *Submission 13*, p.7.

23 OPC, *Guide to handling personal information security breaches*, OPC, August 2008.

24 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41; Ms Alana Maurushat, Cyberspace Law and Policy Centre, *Transcript of Evidence*, 8 October 2009, p.33; Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.5.

25 OPC, *Submission 3, p.*12; OVPC, *Submission 33*, p.8.

26 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1696.

27 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

9.17 A range of submitters endorsed this recommendation as a measure that would mitigate the risks of online fraud.[28] RSA further argued that such a requirement would provide certainty to businesses:

> In addition to alerting consumers to potential loss, such legislation would also provide businesses with a degree of certainty around their responsibilities and the protection of consumer data. Businesses are increasingly vulnerable to potentially serious economic, legal and social repercussions simply because they don't know what is required of them with regard to data breach notification. RSA is asking the Government to provide legislation that provides businesses with greater clarity into their responsibilities, while at the same time protecting the private information of individuals.[29]

9.18 Symantec, whilst supporting mandatory breach notification, cautioned that 'a balanced risk-based approach must be adopted to ensure that organizations and individuals do not find the framework overly burdensome'.[30]

9.19 The Committee heard that the overcollection of data further increases the risks of identity theft and fraud. The OVPC argued that there is an increasing trend for organisations to request personal information during a transaction for purposes unrelated to the transaction, such as marketing and advertising. For example, the OVPC cited the wide use of 'mandatory fields' in electronic forms, where users must submit specific (and sometimes unnecessary) personal information in order to access an online service. The OVPC stated that, as a result of overcollection, personal information held by organisations continues to become more comprehensive, and increases the risk of identity crime following a data breach. The OVPC advocated reducing the amount of information collected by organisations.[31]

9.20 The *Privacy Act* already provides that large organisations may only collect information that is necessary for one or more of its functions.[32] Similar regulations are provided by some State jurisdictions.[33] The ALRC's review

---

28 OPC, *Submission 3, p.*12; OVPC, *Submission 33*, p.8; Symantec Corporation, *Submission 32.1*, p.3; Australian Communications Consumer Action Network, *Submission 57*, p.72.

29 RSA, *Submission 28*, p.4.

30 Symantec Corporation, *Submission 32*, p.11.

31 OVPC, *Submission 33*, pp.5-6.

32 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.710.

33 OVPC, *Submission 33*, pp.4-7.

recommended that public and private organisations alike should be required to only collect information if necessary.[34] The Government accepted this recommendation in the first stage of its response to the review.[35] Dr Bendall, OVPC, supported this move and argued that such provisions could be given further efficacy by removing the exemptions relating to private sector employee records and small businesses mentioned above.[36]

9.21 The OVPC also argued that providing individuals with the option to remain anonymous in online transactions would further reduce overcollection.[37] The *Privacy Act* currently provides a limited right to anonymity in some transactions with large private organisations, but not with government agencies. [38] Legislation exists in some States to extend similar provisions to State government agencies.[39] The ALRC recommended that such regulation be expanded to all private organisations and public agencies so that individuals would have the option to interact anonymously, where lawful and practicable.[40]

9.22 The OVPC supported the proposal for anonymity provisions, and argued that such measures would ensure that 'less information is available to would-be cyber criminals in the event of a data breach'.[41] The ALRC's proposal for an anonymity principal has since been endorsed by the Government.[42]

34 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.732.

35 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.39.

36 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.40.

37 OVPC, *Submission 33*, pp.4-5.

38 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.706.

39 OVPC, *Submission 33*, pp.4-5.

40 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.706.

41 OVPC, *Submission 33*, p.5.

42 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.40.

Consistency among Commonwealth, State and Territory jurisdictions

9.23 Both the OPC and the OVPC argued that the current lack of consistency in privacy legislation among different jurisdictions in Australia represents a gap in privacy regulation and impedes the protection of personal information. Dr Bendall, OVPC, told the Committee:

> South Australia and Western Australia do not have any state based privacy legislation and they do not have an independent regulator. That is often an issue for us when Victorian information is being sent to those jurisdictions. There is a principle in our legislation that Victoria is meant to assure itself that the information is going to be as secure as it would be in Victoria. That is a bit difficult to do that there because there is no law, so it usually has to be done under memorandums of understanding or some other mechanism.[43]

9.24 The ALRC's 2008 review of the *Privacy Act* made recommendations to the effect that Commonwealth, State and Territory governments should agree to form an intergovernmental cooperative scheme to enact consistent legislation in each State and Territory for the handling of personal information.[44] The Government has not currently responded to these specific recommendations.[45] The OPC endorsed the proposal and argued that such a move would 'enhance e-security for information flowing across State and Territory boundaries'.[46]

Industry codes of practice

9.25 As mentioned above, the *Privacy Act* permits organisations to develop and enforce their own privacy codes that replace the National Privacy Principles.[47] Such codes are not widespread, and no such codes currently

43 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, pp.39-40.

44 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.219, 224-225.

45 Department of the Prime Minister and Cabinet, *ALRC Privacy Report*, DPMC, 19 March 2010, viewed 12 April 2010, <http://www.dpmc.gov.au/privacy/alrc.cfm>.

46 OPC, *Submission 3*, pp.9-10.

47 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.263-264.

exist in the telecommunications or information and technology sectors.[48] While larger organisations in these sectors (many of which have detailed privacy policies[49]) are currently regulated under the National Privacy Principles, many smaller businesses that hold large amounts of information, such as small ISPs, are currently exempt from regulation.[50]

9.26 While such gaps in regulation would effectively be bridged by the removal of certain exemptions in the *Privacy Act*, the option also exists for organisations to adopt their own privacy codes to ensure the security of personal information.

9.27 In March 2003, the Internet Industry Association submitted a draft privacy code to the OPC for approval.[51] According to the draft version, the code would apply to IIA members, including small ISPs, who choose to adhere to the code.[52] The code is still currently being considered by the OPC.[53]

International cooperation

9.28 Given that digital personal information is increasingly collected or transferred across international boundaries, the OPC submitted that international cooperation on privacy and data protection is integral to mitigating e-security risks.[54]

9.29 Currently, the provisions of the *Privacy Act* and associated industry codes extend to foreign private organisations handling the personal information of Australian citizens. However, no specific provision exists in the *Privacy Act* to overseas government agencies.[55] The ALRC's review recommended that the *Privacy Act* should be amended to clarify that its provisions also

48 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.264.

49 See for example: Yahoo! Group Australia & New Zealand, *Submission 18*, p.2; PayPal, *Submission 60*, pp.8-9.

50 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, p.1356.

51 IIA, *Privacy Code Draft*, IIA, 2010, viewed 13 April 2010, <http://www.iia.net.au>.

52 IIA, *Internet Industry Privacy Code of Practice Consultation Draft 1.0*, IIA, pp.3-4.

53 OPC, *Privacy Codes Register*, OPC, 2010, viewed 13 April 2010, <http://www.privacy.gov.au>.

54 OPC, *Submission 3*, p.10.

55 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1081-1082.

apply to agencies outside Australia.[56] The Government has accepted this recommendation.[57]

9.30 In addition to these legislative measures, the OPC participates in a number of international forums by which information protection regulators and authorities form partnerships, exchange ideas and pass resolutions on cross-border data protection measures, and privacy issues more generally. These include:

- the Asia Pacific Privacy Authorities forum;
- the annual International Conference of Privacy and Data Protection Authorities;
- the Electronic Commerce Steering Group of the Asia Pacific Economic Community; and
- the Organisation for Economic Cooperation and Development Working Party on Information Security and Privacy.[58]

9.31 Dr Bendall, OVPC, raised concerns that large overseas organisations that retain large amounts of personal information, particularly social networking sites, represent a particular risk to privacy and must be dealt with cooperatively by regulators from different jurisdictions:

> I think [information posted on, and handled by, social networking sites] is a problem for privacy regulators and privacy law, and we are yet to come up with a way of effectively regulating it. It certainly has to be increasingly international. The difficulty is that it is not in one jurisdiction. Often you will be giving your information to a company that is somewhere else. ... those organisations often will claim they can do whatever they like with the information and keep it forever. Even if you cease your Facebook or Youtube site they will still hold the information, so part of it is a conversation with regulators.[59]

9.32 While this discussion may relate to privacy concerns more broadly in relation to social networking, it illustrates the current lack of protection for certain information that is transferred and held overseas. This lack of protection would appear to heighten the risk of identity crime.

---

56 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1104.

57 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.77.

58 OPC, *Submission 3*, pp.10-11.

59 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.45.

Privacy audits

9.33 The *Privacy Act* requires agencies and organisation to take reasonable steps to protect information from unauthorised access, use, modification and disclosure. These steps may include technical measures and organisational processes.[60] Technical measures to protect personal information are examined in Chapter 11.

9.34 Such measures will be particularly pertinent as governments continue to expand the number of services delivered via the Internet, and increasingly exchange and store personal information in digitised form. For example, $467 million of funding was recently announced to form a national e-Health records system.[61] Similarly, the *Government 2.0 Taskforce* has made a number of recommendations encouraging agencies to increase their online engagement with the public.[62] The Committee heard that this growing amount of digitised information, coupled with increased internet speeds, will increase the risks of identity theft and fraud.[63]

9.35 The OVPC suggests that government agencies and private organisations should undertake regular privacy audits to identify breaches of privacy, and risks of such breaches, and to ensure that information is protected at all stages of the information cycle, from collection through to disposal.[64]

9.36 Currently, the OPC encourages, but does not require, government agencies to undertake 'privacy impact assessments' (PIAs) when enacting a new law or starting a new project. Such assessments seek to identify and remedy risks to privacy and personal information during the planning and development stage of such activities. The OPC has not specifically encouraged the use of PIAs by private organisations. The ALRC's review recommended that the OPC should be empowered to direct agencies to provide PIAs on new projects. The ALRC also recommended that the OPC publish guidance on PIAs for organisations and that, in five years, a review should determine if the OPCs directive power should be extended

60 OPC, *Submission 3*, p.6.

61 The Hon Nicola Roxon, *Personally Controlled Health Records for all Australians*, media release, Parliament House, 11 May 2010, viewed 12 May 2010.

62 Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, Australian Government, December 2009, pp.xvii-xviii.

63 AusCERT, *Submission 30*, p.9; Lockstep, *Submission 36*, p.10; ATO, *Submission 59,* p.4; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2.

64 OVPC, *Submission 33*, pp.7-8.

to also cover organisations.[65] The Government has accepted these recommendations.[66]

9.37 Dr Bendall noted that, while PIAs identify initial risks at the beginning of a project, they do not identify risks that emerge after this initial period, nor do they cover existing projects.[67] Dr Bendall stated that the OVPC would like businesses to be encouraged to conduct their own comprehensive regular privacy audits.[68]

Committee View

9.38 The Committee agrees that privacy protections are integral to mitigating the risks of cyber crime. Where personal information is well protected, the scope for identity theft and fraud is reduced.

9.39 The Committee concurs with the recommendations of the ALRC's review relating to preventing over collection. Specifically, requiring agencies and organisations to only collect necessary information would mitigate the effects of data breaches. Similarly, permitting individuals to remain anonymous where lawful and practicable would reduce the amount of information compromised in a data breach. The Committee commends the Government on its acceptance of these recommendations.

9.40 Identity crime risks would be further reduced by ensuring that private sector employee records are sufficiently protected from unauthorised access and disclosure. The removal of the small business exemption would extend protections to a wide range of personal information held by small business. In the case of small ISPs that offer additional services, the removal of the small business exemption would ensure that information that falls outside of the privacy provisions of *Telecommunications Act* is protected. The Committee encourages the Government to accept the related recommendations in the second stage of its response to the ALRC's review.

9.41 To further ensure broad privacy protections, the Committee sees value in the ALRC's recommendations aimed at encouraging the consistency of privacy legislation among Commonwealth, State and Territory jurisdictions.

---

65 ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC, Report 108, May 2008, pp.1569-1570, 1580.

66 Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108*, Australian Government, October 2009, p.86.

67 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41.

68 Dr Anthony Bendall, OVPC, *Transcript of Evidence*, 8 October 2009, p.41.

9.42 Similarly, it is important to ensure that Australian privacy laws extend to foreign agencies and organisations that handle the personal information of Australian citizens and residents. Thus the Committee endorses the ALRC's proposal to extend the *Privacy Act* to cover overseas government agencies.

9.43 The Committee accepts the OVPC's concerns relating to large overseas organisations that hold large amounts of personal information, particularly social networking sites. The Committee recommends that the OPC actively engage with overseas regulators to ensure that these organisations are aware of, and adhere to, Australian privacy laws where appropriate. Where this is not the case, the Committee encourages the OPC to use the full extent of its powers to ensure adherence, including by making, and seeking enforcement of, determinations on complaints against overseas organisations.

Recommendation 28

That the Office of the Privacy Commissioner use the full extent of its powers to ensure that overseas organisations that handle the personal information of Australian citizens and residents are aware of, and adhere to, their obligations under the *Privacy Act 1988* (Cth).

9.44 It is the view of the Committee that individuals should be notified if their personal information is compromised by a data breach. The Committee appreciates the desire of organisations to protect their reputation, however individuals must be empowered to protect themselves from identity theft and fraud. The Committee supports the ALRC's recommendation for mandatory data breach reporting, and encourages the Government to accept the recommendation. The Committee notes that mandatory data breach reporting would also permit more accurate data collection on such incidents.

9.45 Risks of cyber crime would also be reduced by the approval of a code of practice that governs privacy in the Australian Internet industry, including small operators, such as small ISPs. The Committee recognises that the removal of the small business exemption would go some way to extending the provisions of the *Privacy Act* to many currently unregulated members of the industry. However an industry specific code would ensure that the protection of personal information is given an appropriately high priority by the Australian Internet industry, an

industry that handles vast amounts of personal information. The Committee commends the IIA in drafting such a code, and encourages both the IIA and OPC to expedite the adoption of robust and accountable principles. However the effectiveness of such a code in enhancing e-security would depend on the breadth of subscription by members of the Australian Internet industry. Thus adherence to any adopted code by all members is to be encouraged.

Recommendation 29

That the Office of the Privacy Commissioner expedite the adoption of an approved privacy code of practice for members of the Australian Internet industry, including smaller Internet Service Providers.

9.46 Finally, the Committee recommends that private organisations and government agencies should be encouraged to conduct regular audits of existing processes and policies, as well as of new projects, to identify and avoid risks of unauthorised access to personal information. This is particularly important in light of the recent moves by the Government to digitise health records. The Committee recognises the OPC's efforts to encourage the use of PIAs by agencies, and praises the Government's acceptance of the ALRC's recommendations to further encourage the use of PIAs by agencies and organisations. However, the Committee also accepts the concerns of the OVPC that PIAs generally only apply to new projects and laws. Private organisations and government agencies should be required to conduct regular privacy audits of existing data systems, processes and policies, as well as of new projects. This is particularly important in light of a trend toward greater online delivery of commercial and public services. For example, to retain public confidence and minimise e-security risks, any new e-health framework will need strong privacy safeguards, including provision for regular audits of the mechanisms for handling sensitive personal health information.

Recommendation 30

That the Office of the Privacy Commissioner encourage government agencies and commercial organisations to undertake regular audits to identify risks to personal information in both new and existing projects and policies particularly projects that involve the digitisation of large amounts of sensitive information such as the new national e-Health records system.