Australian Government

Office of the Privacy Commissioner

Inquiry into Cyber Crime and its Impact on Australian Consumers

Submission to the House of Representatives Standing Committee on Communications

June 2009

Key Recommendations

1. The Office considers that effective privacy protections in relation to cyber crime (including identity theft[1]) require:

    i. Strong principle-based privacy legislation that minimises the unnecessary collection and disclosure of personal information and enhances the security safeguards surrounding such information.

    ii. Education of government agencies, organisations and individuals to enhance awareness of risks, protections and rights.

    iii. Cross-jurisdictional and cross-portfolio co-operation which recognises that online information flows are not restricted by functional or jurisdictional boundaries, and the consequent risks attached.

    iv. A commitment to the development and implementation of privacy enhancing technologies.

[1] Identity theft involves the illicit assumption of a pre-existing identity of a living or deceased person, or of an artificial legal entity such as a corporation (Australasian Centre for Policing and Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006), 15).

Office of the Privacy Commissioner

2. 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]. The Privacy Act covers 'personal information'. This is defined in section 6 (1) of the Act as information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information.

3. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals.

About this submission

4. The Office of the Privacy Commissioner ('the Office') welcomes the opportunity to provide comments to the House of Representatives Communications Committee in relation to its inquiry into the incidence of cyber crime and its impact on consumers.

5. The Office notes the terms of reference that have been provided for this review of cyber crime and its effects on consumers[3].

6. This submission focuses primarily on the following terms of reference:

   c) level of understanding and awareness of e-security risks within the Australian community.

   d) measures currently deployed to mitigate e-security risks faced by Australian consumers,

   - Education initiatives
   - Legislative and regulatory initiatives
   - Cross-portfolio and inter-jurisdictional coordination
   - International co-operation.

   e) future initiatives that will further mitigate the e-security risks to Australian internet users.

[2] Information relating to the operation of the Privacy Act is available at www.privacy.gov.au.
[3] As at 5 June 2009, the terms of reference for this review were available at http://www.aph.gov.au/House/committee/coms/cybercrime/tor.htm.

f) emerging technologies to combat these risks.

7. This submission highlights the important role played by effective privacy protections in mitigating e-security risks. In doing this, it draws on previous Office submissions to a range of inquiries and consultations, including to the Australian Law Reform Commission's ('ALRC') review of privacy law in Australia[4].

8. This submission also provides an overview of research conducted on behalf of the Office on community understanding of e-security risks. It also discusses current privacy protections against cyber crime and opportunities to enhance these protections.

Level of understanding and awareness of e-security risks within the Australian Community

9. The Office regularly commissions surveys on community attitudes to privacy in Australia. The most recent survey conducted in August 2007 included questions about community attitudes towards 'privacy and the internet' and 'identity fraud and theft'[5]. Identity fraud and theft was defined as 'where an individual obtains personal information (e.g. credit card, drivers licence, passport or other personal identification documents) and uses it to fraudulently obtain a benefit or service for themselves.

10. The key findings in relation to privacy and the internet included:

- 50% of respondents were more concerned about providing information over the internet than they were two years earlier, with 31% as concerned and 11% less concerned. A higher proportion of respondents aged under 24 claimed to be less concerned than other age groups[6].

- 65% of respondents felt more concerned about providing details online compared to providing details in hard copy format[7].

- 25% of respondents claimed that they provide false information in online forms as a means of protecting their privacy. 58% of respondents aged between 18 and 24 years reported providing such false information[8].

11. The key findings in relation to identity fraud or theft included:

[4] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (http://www.austlii.edu.au/au/other/alrc/publications/reports/108/).
[5] Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007) (http://www.privacy.gov.au/publications/rcommunity07.pdf). Information about the survey design is available at http://www.privacy.gov.au/publications/rcommunity07methodology.pdf.
[6] *Community Attitudes Towards Privacy 2007*, paragraph 12.1.
[7] Ibid, paragraph 12.1.
[8] Ibid, paragraph 12.2.

- 96% of respondents said that identity fraud or theft is an invasion of privacy[9].

- 60% of respondents were 'concerned' or 'very concerned' about becoming the victim of identity fraud or theft. Respondents living in middle income households ($25,000 - $100,000) were the most concerned[10].

- 9% of respondents claimed they had been the victim of identity fraud or theft and 17% claimed to know someone who had been the victim. The likelihood of being a victim was highest among people working in upper white collar professions and among those aged between 25 and 49[11].

- 45% of respondents considered that identity fraud and theft could most easily occur through online activities (e.g. using the internet in general, buying items online and online banking). Concerns about the possibility of identity fraud and theft over the internet increased with increasing levels of income[12].

Legislative and regulatory initiatives to mitigate e-security risks

12. The Privacy Act provides high-level principle-based regulation that is technologically neutral. This is primarily codified in 11 Information Privacy Principles ('IPPs') that apply to Australian and ACT Government agencies, and 10 National Privacy Principles ('NPPs') that apply to many private sector organisations.

13. The effect of this regulation is to create general rules for the handling of personal information. This includes how personal information may be collected, used, disclosed and stored. In addition, each set of principles creates rights for individuals to access personal information about them and where necessary, have it corrected.

14. In the Office's view, these principles (some of which are outlined below) assist in mitigating e-security risks.

15. For example, IPP 1 provides that an agency may not collect personal information unless that information is necessary for, or directly related to, a function or activity of the agency. The Privacy Act also imposes similar, though not identical, obligations on many private sector organisations. NPP 1 precludes an organisation from collecting personal information unless it is necessary for one or more of its functions or activities.

[9] Ibid, paragraph 13.0.
[10] Ibid, paragraph 13.1.
[11] Ibid, paragraph 13.1.
[12] Ibid, paragraph 13.2.

16. In the Office's view, these collection principles minimise the amount of personal information that agencies and organisations may collect, limiting the potential for unnecessary information to be handled inappropriately.

17. IPP 11 provides that an agency may not disclose personal information held in a record to another person, body or agency unless a specified exception applies. NPP 2.1 also limits the circumstances in which an organisation may disclose an individual's personal information. It provides that an organisation may not use or disclose an individual's personal information for a purpose other than the primary purpose of collection unless a specified exception applies.

18. The Office considers that these disclosure principles assist to mitigate e-security risks by limiting the opportunity for personal information to be inadvertently disclosed to a person who may use it for malicious purposes.

19. IPP 4 establishes obligations on agencies to have in place security safeguards, as are reasonable in the circumstances, to protect personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse. NPP 4 requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure.

20. In both IPP 4 and NPP 4, what constitutes 'reasonable steps' to protect personal information will depend on the agency's or organisation's particular circumstances, the sensitivity of the information in question, and the harm likely to result if the information is not secure. Reasonable steps may include computer and network security, such as strong encryption, access controls (both physical and logical), anti-virus, spyware and malware protections, firewalls, and audit trails. Internal policies and processes, staff training and measures to promote an appropriate organisational culture are also important elements to an effective security regime.

21. NPP 9 generally requires organisations to take reasonable steps to ensure that the information transferred overseas will be afforded protections substantially similar to those in the NPPs unless a specified exception applies.

22. Given the increasing ease with which information can be transferred between countries, the Office considers that NPP 9 helps Australians to feel confident that if their personal information is transferred overseas, it will be subject to privacy protection to the same standard enjoyed in Australia. There is no similar principle in the IPPs. However, all disclosures made by Australian Agencies, including disclosures overseas must be made in accordance with IPP 11.

23. In addition, the Office notes that many Australian Government agencies are subject to agency-specific legislative requirements that add further

privacy protections (such as secrecy provisions), as well as other requirements which apply more generally across government. Such measures appropriately provide protections in addition to those in the Privacy Act where privacy and security risks are greater.

Educational initiatives to mitigate e-security risks

Agencies and organisations

24. The Privacy Commissioner has responsibility under the Privacy Act to promote privacy by developing educational and guidance materials that explain agencies' and organisations' obligations under the Act and that suggest practices to avoid adversely impacting on individuals' privacy[13]. Some recent examples of educational materials released by the Office are outlined below.

25. In February 2009 the Office commissioned ORIMA Research to undertake the first online survey of Australian Government agencies to identify how they have addressed the use of both agency-issued and privately owned portable storage devices in the workplace. The Office had identified that portable storage devices including USB sticks, laptops and personal digital assistants presented privacy risks due to their small size and large storage and functional capabilities. These privacy risks include that personal information stored on a portable storage device may be compromised through the operation of malicious software or the device may be lost or stolen.

26. The Office released the results of the survey in Privacy Awareness Week 2009 (3 – 9 May 2009). The results suggested that agencies are generally doing well at managing personal information stored or handled on portable storage devices but that there was room for improvement.

27. To help agencies better manage these privacy risks the Office released a *Public Sector Information Sheet 3: Portable Storage Devices and Personal Information Handling*[14]. This was also intended to assist agencies to comply with storage and security obligations in IPP 4(a).

28. During Privacy Awareness Week 2008 (24 – 30 August 2008), the Office released a *Guide to Handling Personal Information Security Breaches*[15]. The Guide sets out key steps and factors for agencies and organisations to consider when responding to a personal information security breach. These include containing the breach and conducting a preliminary

[13] Sections 27 (1) (d) and (e) of the Privacy Act.
[14] See *Portable Storage Devices and Australian Government Agencies: Personal Information Survey April 2009* available at http://www.privacyawarenessweek.org/paw/info_sheet3_psd.html) and *Public Sector Information Sheet 3: Portable Storage Devices and Personal Information Handling* available at http://www.privacyawarenessweek.org/paw/info_sheet3_psd.html.
[15] See http://www.privacy.gov.au/publications/breach_guide.html.

assessment, evaluating the risks associated with the breach, considering whether to notify those affected by the breach and preventing further breaches from occurring.

29. These measures aim to help agencies minimise the adverse impacts of a security breach, including where appropriate, by giving individuals an opportunity to take steps to protect their interests.

30. Finally, in August 2007 the Office released an information sheet for private sector organisations titled *Private Sector Information Sheet 20- Scanning 'Proof of Identity' Documents*[16]. The Office considers that scanning technology poses a risk to the security of individuals' personal information because once personal information has been scanned, it becomes digitised and may be used or disclosed for many other purposes including financial, credit card or identity fraud. The information sheet explains organisations' obligations under the NPPs in relation to personal information collected using scanning technology.

Individuals

31. The Office considers that measures which empower individuals to protect themselves in online and IT-enabled environments are essential to promoting effective privacy and e-security.

32. The Privacy Commissioner has the responsibility of protecting individuals' privacy by undertaking educational programs either solely or in co-operation with other parties[17].

33. For example, the Office promotes secure and safe online behaviour and secure information exchange by advising on social networking, online privacy tools and internet privacy. Much of this information has been provided to individuals in a series of 'frequently asked questions'[18].

34. The Office has also developed a Youth Portal, released during Privacy Awareness Week 2009 which is a forum for young people to learn about current privacy issues. The portal includes *private i - Your ultimate privacy survival guide* and a short animated video, *Your Privacy is Important. Think Before You Upload!* (a joint initiative of the Asia Pacific Privacy Authorities). These publications highlight the possible risks of using online technologies such as social networking and gaming sites and suggest how young people may protect their personal information when accessing these technologies[19].

35. The Office considers that individuals are also empowered when they are aware of their rights and those rights are easily accessible. In this regard

[16] See http://www.privacy.gov.au/publications/IS20_07.html.
[17] Section 27 (1) (m) of the Privacy Act.
[18] The Office's 'Frequently Asked Questions' page is available at http://www.privacy.gov.au/faqs/ypr/index.html.
[19] See http://www.privacyawarenessweek.org/topics/youth/index.html.

the Office provides detailed guidance to individuals on how to make complaints about practices which may be an interference of privacy under the Privacy Act[20]. This guidance is accessible to individuals with non-legal or technical backgrounds and is also provided in 11 languages other than English[21].

Cross-portfolio and inter-jurisdictional coordination to mitigate e-security risks

36. The flow of online information is not confined by functional or physical boundaries, but takes place across various levels of government, the private sector and different jurisdictions.

37. In the Office's view, an important way to mitigate e-security risks associated with this information flow is to adopt a coordinated approach across portfolios and jurisdictions.

38. Cross-portfolio co-operation enables agencies specialised in particular areas to collectively consider different aspects of information communications technology initiatives and their associated privacy and security risks, and to develop an appropriate response.

39. The Office regularly engages with agencies on a wide range of projects which potentially impact on the flow of individuals' personal information. For example, the Office participates in the development of the National Identity Security Strategy ('NISS'), which provides an important cross-jurisdictional forum for the development of strong identity security and management. The Office is also actively involved in a cross-portfolio working group chaired by the Australian Government Information Management Office ('AGIMO') in relation to online authentication issues.

40. Recently the Office provided privacy advice and assistance to the Department of Broadband, Communications and the Digital Economy (DBCDE) in relation to setting up a youth online forum. As a result of DBCDE's successful introduction of the forum, the Office is now developing guidance for other agencies that facilitate similar online forums.

41. The Office also contributes to inter-jurisdictional forums, such as the Privacy Authorities Australia ('PAA') forum, to adopt a co-ordinated approach to issues affecting individuals' personal information.

42. The PAA forum is made up of state, territory and federal privacy authorities. This collaborative forum, which meets biannually, discusses issues of common interest, including privacy law reform and technology advances and their impacts on privacy.

[20] See http://www.privacy.gov.au/privacy_rights/complaints/index.html.
[21] See http://www.privacy.gov.au/privacy_rights/languages/index.html.

43. Notwithstanding this inter-jurisdictional co-operation, a significant issue in privacy regulation in Australia is the need for greater consistency, simplicity and clarity between jurisdictions. Currently, the privacy protections afforded to personal information may vary significantly as it is exchanged between jurisdictions.

44. The Office therefore supports achieving national uniformity in privacy regulation, as recommended by the ALRC in its review of privacy law[22]. The Office considers that greater consistency in privacy regulation would enhance e-security for information flowing across State and Territory boundaries.

International co-operation to mitigate e-security risks

45. In the Office's view, an important component of mitigating e-security risks is to recognise the international cross-jurisdictional nature of online information flows, and to foster international co-operation on privacy and data protection.

46. The Office has recognised the importance of actively and constructively engaging with privacy and information protection regulators in other nations and economies. For example, the Office is a member of the Asia Pacific Privacy Authorities ('APPA') forum. APPA is the principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. APPA membership includes similar regulators from other Australian jurisdictions, as well as New Zealand, Hong Kong, South Korea and Canada, including both the Federal Office and the province of British Columbia[23].

47. The Office also actively participates in the annual International Conference of Privacy and Data Protection Authorities[24].

48. In addition, the Office, through the Australian Government, is an active participant in the work being progressed by the Electronic Commerce Steering Group of the Asia Pacific Economic Community ('APEC'). The primary outcome of this work has been the APEC Privacy Framework and Principles.

49. The APEC Privacy Framework aims to promote a consistent approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows. The aim is to have protections consistent across the region which in the

[22] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 3-4, recommendation 3-5, recommendation 3-6.
[23] See http://www.privacy.gov.au/international/appa/index.html.
[24] For information on these annual conferences see http://www.privacy.gov.au/links/index.html#12.

Office's view will help to mitigate e-security risks as well as assisting business and member economies to be at the forefront of e-commerce.

50. Through DBCDE, the Office has also engaged with the Organisation for Economic Cooperation and Development's (OECD) Working Party on Information Security and Privacy (WPISP). The Office has provided input into the development of a WPISP 'primer' for policy makers on the management and protection of digital identities and will continue to engage in the identity management work as well as other initiatives the working party undertakes in the area of privacy.

Future initiatives that will further mitigate the e-security risks to Australian internet users

51. In its review of privacy law the ALRC made a number of recommendations which if adopted, could further mitigate the e-security risks faced by Australian internet users.

52. These recommendations included:

- **Unified privacy principles** – The ALRC recommended that the existing two sets of privacy principles in the Privacy Act should be consolidated to a single body of regulation that applies equally to the private sector and Australian Government agencies[25]. As part of this consolidation, the ALRC recommended that a cross-border data flow principle should apply to organisations and agencies. This would generally provide that an agency or organisation remains accountable for personal information it transfers overseas (subject to any applicable exception)[26].

  The Office supports this recommendation and considers that it would reduce regulatory complexity and promote understanding and compliance with privacy obligations.[27]

- **National uniformity** – As noted above, the ALRC recommended achieving national uniformity in privacy regulation.

- **Mandatory breach notification** – The ALRC recommended that the Privacy Act should be amended to require an agency or organisation to notify the Office and affected individuals of a data breach in certain circumstances[28].

  The Office supports the introduction of mandatory notification obligations where a breach of personal information security may pose

[25] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 18-2.
[26] Ibid, recommendations 31-1 and 31-2.
[27] See the Office's response to the ALRC's Discussion Paper 72, proposal 3-2, available at http://www.privacy.gov.au/publications/alrc211207.html.
[28] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 51–1.

a real risk of serious harm to an individual. In the Office's view, this would allow individuals to take tangible steps to protect their interests[29].

- **Guidance on online privacy** – The ALRC recommended that the Office, in consultation with the Australian Communications and Media Authority, should ensure that specific guidance on the privacy aspects of using social networking sites is developed and incorporated into publicly available education material[30]. The ALRC also recommended that State and Territory education departments should incorporate education about privacy and, in particular privacy in the online environment, into school curricula[31].

  The Office agrees with these proposals in principle, and welcomes and encourages initiatives which bring the research community together with other key education stakeholders to deepen understanding of key and emerging issues and educational needs facing young people[32].

- **Guidance on generally available publications** – The ALRC recommended that the Office should develop and publish guidance on generally available publications available in electronic form[33].

  The Office supports this recommendation, which reflects the new conditions under which records may now be made public in electronic form. These conditions include that data from electronic records can be retrieved, matched and aggregated with relative ease, and may be broadly disseminated via the internet[34].

53. The Office understands that the Australian Government is currently preparing a response to the ALRC's report.

New technologies to combat e-security risks

54. As noted in its submission to DBCDE on the Future Directions consultation Paper, the Office supports the development of privacy enhancing technologies.[35] These technologies illustrate the important role of technology in supporting privacy and e-security. They achieve this by meeting security and other objectives, while at the same time providing

[29] This is discussed in the Office's response to Chapter 47 of the ALRC's Discussion Paper 72 available at http://www.privacy.gov.au/publications/alrc211207.html.
[30] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 67-3.
[31] Ibid, recommendation 67-4.
[32] This is discussed in the Office's response to Chapter 59 of the ALRC's Discussion Paper 72, available at http://www.privacy.gov.au/publications/alrc211207.html.
[33] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 11-1.
[34] This is discussed in the Office's response to Chapter 11 of the ALRC's Issues Paper 31 available at http://www.privacy.gov.au/publications/alrc211207.html.
[35] See http://www.privacy.gov.au/publications/sub_broadband_digital_economy.html

individuals with appropriate control and choice over how their personal information is handled. [36]

55. Privacy enhancing technologies tend to fall into several categories and can be aimed at individual or organisational use, for example:

- **General information security tools** such as encryption, logical access controls, use of digital certificates etc.
- **Data separation** which refers to systems that detach identifying information from other personal information so that the privacy of the individual is protected during processing and storage of their personal information; generally only an authorised person with a digital key is able to re-identify information.[37]
- **Privacy metadata** refers to information 'tags' that can be attached to personal information during processing. These tags contain additional information such as: the source of the information, the consent obtained, how it may be used and the policies to which it is subject. Personal information can also be assigned particular conditions or 'obligations' which detail the length of time that information may be retained and whether the person has given consent for the information to be disclosed to any third parties.[38]
- **Privacy management systems** are systems that allow individuals to find out the privacy practices or processing policies of organisations that handle personal information and see if these match their preferences. These systems can improve the transparency of the information processing for the individual.[39] Some examples of privacy management systems include P3P and IBM's secure perspective software. As the UK Information Commissioner has pointed out, these tools '...may also advise users of the consequences of the information processing performed leading to an improved understanding of privacy-related issues.'[40]
- **Anonymising tools** include tools that hide the IP address or email address of the individual. Other similar privacy enhancing technologies in this category include those that allow anonymous or pseudonymous payment where the individual purchases a pre-paid card to make payments online.[41] Organisations can also build in anonymity or

[36] Privacy enhancing technologies are discussed in greater detail in *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* and published by the Dutch Government, www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.
[37] See *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* and published by the Dutch Government, www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.
[38] UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx.
[39] *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* published by the Dutch Government www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf
[40] UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx.
[41] UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx.

pseudonymity options into digital systems where full identification is not necessary. With options for anonymous transacting in place, organisations will be better able to meet their obligations under the Privacy Act which require that: 'Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.'[42]

56. The Office submits that a commitment to the development and implementation of privacy enhancing technologies should form a key element of the Australian Government's work to reduce e-security risks while providing Australian consumers with appropriate control and choice over the handling of their personal information.

[42] National Privacy Principle 8, Schedule 3, *Privacy Act 1988*.