Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to House of Representatives Standing Committee on Communications

on its

Inquiry into Cyber Crime

July 2009

Table of Contents

The Privacy Commissioner wishes to acknowledge the work of Scott May (Policy and Compliance Officer) in the preparation of this Submission.

Office of the **Victorian Privacy Commissioner** (Privacy Victoria)
GPO Box 5057
10-16 Queen Street
Melbourne Victoria 3000
Australia
Phone: 1300-666-444
Fax: +61-3-8619-8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

1. Introduction

The development and popularity of e-commerce and online transactions have grown exponentially during the 'Information Age', and are set to continue.[1] This growth has brought with it many benefits, such as convenience for consumers and reduced transaction costs for business and government. With annual e-commerce transactions totalling into the billions of dollars, it is to be expected that criminal groups are attracted to the potential gains of cyber crime, including identity theft and financial fraud. The future growth success of e-commerce is dependent on consumers having faith in the security of such technology.[2]

Educative campaigns generally concentrate on individual consumers, for example, urging consumers not to make their personal information freely available on social networking sites. Whilst this approach is to be encouraged, a great deal of the personal information available in society is held by organisations.[3] Databases of government authorities and large corporations contain the most accurate, sensitive and valuable personal information. Organisational databases are attractive to cyber criminals, given the breadth and depth of information they contain. Access to such databases, or access to excerpts of them, allows for the total assumption of an identity of an individual and/or large scale commercial fraud.

2. Executive Summary

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. The information can be acquired from an individual directly, but also by attacks on the data security of organisations. Actions by both public and private organisations, which protect the privacy of individuals, will reduce the likelihood and incidence of cyber crime.

This submission will focus on measures to enhance and strengthen privacy protection within Australia, thereby minimising the risk and mitigating e-security risks faced by Australian consumers.[4] I recommend increasing the breadth, scope and strength of privacy laws in Australia, and this submission will discuss measures organisations can take to further fortify data security within their organisation.

Summary of Recommendations to address cyber crime through privacy laws:

Closure of existing gaps within Australia's legal privacy framework, in both statute and common law.

Individuals transacting online are informed of the opportunity to transact anonymously where possible.

Organisations do not request or record personal information when not necessary for the interaction/transaction with the organisation.

Where an organisation requires collection of personal information, the organisation collects only the absolute minimum necessary for the purposes of the interaction.

Organisations should review forms and websites, particularly those with mandatory fields, to ensure information sought from consumers is actually required for the purposes of the interaction.

Data Security principles are maintained over the life-cycle of the data, and staff are appropriately trained in such principles.

Organisations ensure data is only accessed by employees/contractors on a 'need to know' basis.

Encryption of data is encouraged, both within and outside organisations.

Organisations regularly conduct audits of information held, to identify existing or potential breaches.

Organisations notify potential victims and the relevant privacy regulator of potential or actual data losses or privacy breaches, where there is a reasonable belief the data loss or privacy breach may lead to financial fraud or identity theft.

3. Australian privacy law – legislative framework

a) Existing legislative landscape – Commonwealth and Victoria

Existing Australian privacy laws focus primarily on the organisations which are purported to be regulated. The *Privacy Act 1998 (Cth)* regulates information held by the Commonwealth public sector, as well as most corporations and credit providers.[5] The substantive requirements contained within the *Privacy Act* are known as the 'Information Privacy Principles' (for federal Government organisations) or the 'National Privacy Principles' (applying to private sector organisations). These principles cover actions relating to collection, use and disclosure, transborder data flows, and data quality and security of personal information.[6]

In Victoria, in the absence of any conflicting laws, the *Information Privacy Act 2000 (Vic)* ('IPA') regulates all Victorian public sector organisations as well as service providers acting under a Victorian public sector contract.[7] The IPA regulates protection of information privacy, and provides individuals with a complaint mechanism.[8] The requirements in the IPA, known as 'Information Privacy Principles', are similar in substance to the *Privacy Act's* 'National Privacy Principles'.[9] Additionally, the Victorian *Charter of Human Rights and Responsibilities Act 2006 (Vic)* requires public authorities to act in ways compatible with the rights contained in the charter, which includes a right to privacy.[10]

b) Existing privacy laws – Other Australian states and territories

Other Australian jurisdictions have similar privacy obligations enshrined in legislation (as in Victoria) or have an administrative system of privacy protection.

New South Wales, the ACT, Tasmania, Queensland and the Northern Territory have all implemented their own privacy legislation regulating their respective public organisations. Each jurisdiction maintains separate privacy regulators to oversee compliance with their individual Acts.[11]

South Australia and Western Australia currently have no privacy-specific legislation. However, South Australia maintains an administrative scheme of privacy protection, but without an independent regulator.[12]

c) Gaps within the current legislative privacy framework

Gaps in the coverage of privacy laws exist within Australia. These relate to the scope and coverage of privacy protection. Of most significance are the areas of workplace privacy, and the existing small business exemption.

The Victorian Law Reform Commission found 'significant' gaps in the protection of privacy in the workplace.[13] Employee records are specifically excluded from the federal *Privacy Act.*[14] Such records, particularly of large corporate employers, contain vast amounts of employee personal information, and such information remains unprotected under privacy legislation.[15]

'Small' businesses, defined as businesses with an annual turnover of less than $3 million, are exempt from the application of the *Privacy Act.*[16] This means smaller businesses (which may hold significant personal information) need not comply with privacy principles, and the protection of personal information held is at the whim of each small business. The Australian Law Reform Commission (ALRC) estimates that 94% of Australian businesses fall under the 'small business' definition, meaning the exemption provides a significant gap in the protection of privacy within Australia.[17]

The ALRC has recommended closure of both of the above gaps and the adoption of consistent, uniform privacy regulation.[18]

d) Lack of Common Law protection

Whilst the above legislative provisions provide limited support for privacy within Australia, individuals acting in their own capacity have no obligations under any privacy legislation.

Additionally, there is currently no common law action for breach of privacy in Australia. Other common law actions (defamation, breach of confidence, nuisance and trespass)[19] have been used to partially protect limited privacy rights. Whilst the Victorian Court of Appeal has awarded damages for mere distress for breach of confidence, it did not decide on the validity of a 'tort of privacy'.[20]

The ALRC has recommended establishment of a statutory cause of action for breach of privacy.[21] A statutory cause of action would confer obligations on individuals and expand the protection of privacy within Australia.

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.

4. Anonymity

a) Current legislation

In dealing or interacting with organisations, individuals should be afforded the opportunity to remain anonymous where possible. All Victorian public sector organisations,[22] as well as some private sector organisations,[23] are currently required

to provide individuals with the option of not identifying themselves when entering into a transaction when it is lawful and practicable to do so.[24]

The option of not identifying oneself restricts the personal information that is communicated to and retained by the organisation. Less information is available to would-be cyber criminals in the event of a data breach.

b) Australian Law Reform Commission recommendations on Anonymity

The ALRC recommended that the ability of individuals to remain anonymous when interacting with organisations be incorporated as the first principle of its model Uniform Privacy Principles (UPP). The fact that the ALRC recommended anonymity be the first principle underlines its importance. The ALRC has stated that anonymity 'is an important component of the model UPPs.' The proposed model UPP 1 states: [25]

> **UPP 1: Anonymity and Pseudonymity**
> Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:
> (a) not identifying themselves; or
> (b) identifying themselves with a pseudonym

The ALRC further recommended all agencies and organisations 'accommodate the (anonymity) principle through their privacy policies'.[26]

However, few individuals are aware of their ability to remain anonymous and disclose personal information when it is not required, for example, when receiving general advice from an organisation. Organisations should not encourage the solicitation of personal information, or recording of it, when it is not required by the organisation.

c) Societal and Legislative opposition to Anonymity

The last decade has seen a surge in the requirement for individuals to identify themselves. A flurry of national security related legislation has been implemented in the last decade,[27] much of which authorises and encourages the collection of information for various purposes.[28] National security campaigns implore the community to assiduously report information, as 'every detail helps.'[29] For example, the *Anti-Money Laundering and Counter-Terrorist Financing Act 2006 (Cth)* requires 'reporting entities' to actively collect personal information and report certain information about their customers to the relevant authority.[30]

Such legislative change has brought about fierce legal and societal debate surrounding anonymity. Anonymity is often viewed as implying 'something to hide' or even criminal connotations. Corporations continue to submit that anonymity is unnecessary.[31] However, surveys indicate strong community support for anonymous interaction.[32] There is a variety of legitimate reasons why individuals may wish or need to remain anonymous, and individuals should not feel the need to 'justify' such a request. Individuals should be informed of their ability to transact or interact anonymously with and organisation, where appropriate.

5. Over-collection of Personal Information

The most privacy protective method of handling personal information is not to collect it at all. Personal information that is not collected cannot be subsequently disclosed, misused or lost, and cannot lead to a potential identity theft or identity-related financial fraud.

a) Current Legislation

Current Australian privacy legislation contains provisions relating to the collection of personal information. The Victorian *Information Privacy Act* and Commonwealth *Privacy Act* requires Victorian and Commonwealth public sector organisations, as well as private sector organisations subject to the *Privacy Act* 'must only collect personal information that is necessary for its functions or activities'.[33]

b) Practice of Over-collection

It is common practice for organisations to 'over collect' the personal information of individuals interacting with them. Over-collection leaves organisations open to larger and more damaging consequences when the security of a database is breached.[34] The more comprehensive the personal information collected, the more valuable it will be to those wishing to commit fraud.

c) Use of Mandatory Fields

One common area of over-collection is the use of mandatory fields. This approach is increasingly common in an online environment when organisations interact with the public. Organisational web sites often contain mandatory fields, stating information is required or necessary for a user to access a service or interact with the organisation. Often end users will simply fill out the form without turning their minds to the necessity of the collection of information.

Most problematic is when the web site refuses users to progress past the form without filling in the mandatory requirements. Whilst paper-based form users may simply refuse to fill in requests for information (and in Australia routinely do[35]), such an option is unavailable online, effectively forcing consumers to provide information in order to access a required service.

It is questionable whether organisations actually do require, in each instance, the personal information requested in necessary or required fields. Such forms are often of a 'standard' type, generally erring on the side of over-collection, and thus collect more personal information than required for the actual interaction requested.

d) Danger of Over-collection

Collection of some personal information by organisations will be necessary, for example, to verify identity. However, there is a worrying trend for organisations to request personal information for essentially unrelated purposes, such as marketing, statistical, advertisement or even profit-driven motives.[36] As a result, personal information held by organisations tends to expand over time, becoming increasingly comprehensive.

In the event of a data-security breach, the 'wealth' of personal information lost or disclosed is likely to be broader, and the potential for fraud or identity theft arising from the data loss is subsequently increased.

In short, government and private organisations should only collect personal information that is necessary for their functions. Such a change in approach may be a radical one for organisations which currently collect as much personal information as possible from individuals who interact with them. However, such a change is a privacy protective one, and a necessary approach to addressing cyber crime.

6. Data Security

Organisations should take adequate steps to prevent loss or unauthorised disclosure of personal information that is necessary to collect. Data security, including the level of protection afforded, should be consistent throughout the life-cycle of the data.[37]

Organisations often devote significant time and resources to the prevention of cyber-interception or 'hacking', viewing cyber crime as a purely technological issue.[38] Whilst important, technological actions alone will not suffice.

a) Organisational and behavioural practices

Whilst technical controls to prevent attacks on data security are to be encouraged, organisational processes post-collection should not be overlooked. Organisations 'readily disseminate the personal information...to a host of other entities', such as through the sale of personal data.[39] Data security can be compromised through 'relatively low-tech means' including unauthorised employee action.[40] The US Federal Trade Commission has noted 'strong growth' in 'insider threats', such as employees transferring data to identity thieves.[41] Organisations should implement workplace policies that maintain the security of data from collection to disposal, and ensure computer security infrastructure reflects this approach across the entire organisation.[42]

b) User Access Control

One method of reducing the chance of data loss is ensuring strict access controls on personal information databases within the organisation. Access should only be granted to users who actually require access to the data to perform their set tasks or duties on a 'need to know' basis.[43] A variety of technical options and standards are available for organisations to implement user access control.[44]

c) Encryption

Another measure for minimising information loss is ensuring the encryption of data when it is used within or transferred outside the organisation. There are multiple instances of unencrypted storage devices, such as laptops, being misplaced or lost.[45] Encryption of data and devices makes access increasingly and prohibitively difficult for potential identity thieves to gain access to the data. Failure to encrypt data and carelessness 'down the chain' of the data lifecycle will subvert the most secure technological developments.[46]

d) Audit control and procedures

E-security risks such as identity crime often remain unknown until manifested in a fraudulent transaction. One method of anticipating such risks is to conduct proactive auditing procedures. Such procedures enable organisations to find out whether privacy breaches or data loss has occurred, or where and when it is likely to occur, and to take steps to reduce the level of risk. Audit procedures should focus on 'event logs and related activities...to determine adequacy of current system measures...the degree of conformance with established policy, and recommend improvements to current measures'.[47]

e) Automatic notification of privacy breach/data loss

Once an organisation is aware of a breach of data security, it can take steps to reduce the likelihood of an identity crime occurring against the individuals whose personal information has been compromised. One such method is mandatory notification, which requires organisations to notify potential victims of the circumstances surrounding a breach that has occurred. This provides at-risk individuals the opportunity to take steps to protect or change personal information.

The ALRC recommended amendment of privacy laws to include breach notification to the Office of the Privacy Commissioner and potential victims.[48] Whilst notification is not required under current privacy legislation, it is good practice for organisations to do so.[49]

7. Conclusion

Educational and regulatory efforts should focus on the collection and data security of personal information held by organisations in both the public and private sectors. By reducing the amount of personal information collected by organisations, the potential for identity theft when data is lost or disclosed is minimised. When an organisation must collect personal information, they should ensure the security of the information retained from collection to disposal.

Whilst measures to mitigate e-security risks such as 'Trojan horses' are to be encouraged and applauded, such measures alone will be insufficient. 'Even a fortress with impenetrable walls is hardly secure if the back gate is left open'.[50] Organisations must be encouraged to make information privacy a higher priority than it has previously attained.

HELEN VERSEY
Victorian Privacy Commissioner

8. Endnotes

[1] Online sales growth is predicted to be 14% annually, despite current economic conditions, for the next 5 years. Johnston, C. *US eCommerce: 2005 to 2010 – a 5 year forecast and analysis of US online retail sales,* <http://www.forrester.com/Research/Document/Excerpt/0,7211,37626,00.html> accessed at 17 June 2009.
[2] For example, UK surveys identify that one in three Internet users refuse to shop online. Office of Fair Trading (UK), 'More to do to improve consumer trust online', (Press Release, 11 May 2009). http://www.oft.gov.uk/news/press/2009/52-09
[3] 'Submission to Standing Committee on Access to Information, Privacy and Ethics', Parliament of Canada, Ottawa, 8 May 2007, < http://www.privcom.gc.ca/parl/2007/sub_070508_e.cfm>
[4] The Office of the Privacy Commissioner has argued "Many of the privacy breaches that (the OPC) is aware of occurred not only because of malicious activity by hackers and crime groups, but also as a result of organisations failing to adopt sound privacy policies and practices aimed at preventing data loss or leakage." Office of the Privacy Commissioner, 'Media release: Better e-security is key to enhanced privacy" (Press Release, 6 June 2008).
[5] But only corporations with over $3m annual turnover, See *Privacy Act 1998 (Cth)* s.6D and for credit providers, Part IIIA.
[6] See *Privacy Act 1998 (Cth)* Sch 2.
[7] *Information Privacy Act 2000 (Vic)* s.9.
[8] See s.6 and s.25, *Information Privacy Act 2000 (Vic)*
[9] For example, compare *Privacy Act 1988 (Cth)* Sch 3 with *Information Privacy Act 2000 (Vic)* Sch 1.
[10] *Charter of Human Rights and Responsibilities Act 2006 (Vic)* s.13, specifically that 'a person has the right not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with'.
[11] In NSW, see: *Privacy and Personal Information Protection Act 1998 (NSW),* In ACT and NT see: *Privacy Act 1988 (Cth),* In Tasmania see: *Personal Information Protection Act 2004 (Tas).* In Queensland, *Information Privacy Act (Qld) (2009).*
[12] See Privacy Victoria, *Privacy and Related Legislation in Australia* (2008) http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/8219B55BB38A8CBBCA256F8C00209B48/$FILE/Privacy%20and%20related%20legislation%20in%20Australia%20at%205%20October%202008.pdf at 29 June 2009.
[13] Victorian Law Reform Commission, *Workplace Privacy Final Report*, Report No 159 (2005) [1.25].
[14] *Privacy Act 1988 (Cth)* s.7B(3).
[15] However, as the Victorian *Information Privacy Act* contains no such exemption, Employee records are covered for organisations subject to the IPA.
[16] *Privacy Act 1988 (Cth)* s.6D.
[17] Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [2.20].
[18] Australian Law Reform Commission, '*For your information: Australian Privacy Law and Practice'*, Report No 108 (2008) Rec 3.1.
[19] See Paras 55 and 56, Office of the Victorian Privacy Commissioner, *Submission to the Victorian Human Rights Consultation Committee on its inquiry into 'A Charter of Human Rights for Victoria',* (2005).
[20] See *Giller v Procopets* [2008] VSCA 236.
[21] ALRC, above n 17, Rec 74.
[22] *Information Privacy Act 2000(Vic)* s.9.
[23] *Privacy Act 1988 (Cth)* s.6C.
[24] *Information Privacy Act* 2000 (Vic), Sch 1, IPP 8.1.
[25] ALRC, Above n 18, [20.41] and [20.71].
[26] ALRC, Above n 18, [20.45].
[27] For example, see Attorney-General's Department, *Australian National Security: What Governments are doing,* (2009). <http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D49EA90CA256FAB001BA5EA?OpenDocument>
[28] For example, see *The ASIO Legislation Amendment Act 2003* (Cth).
[29] Attorney-General's Department, Above n 27.
[30] *Anti Money Laundering and Counter Terrorism Financing Act 2006 (Cth)* s.4.
[31] For example, see Telstra's submission stating anonymity "would add to an already heavy compliance burden for organisations", ALRC Above n 18, [20.59].

[32] For example, "A series of surveys conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability (GVU) Centre repeatedly demonstrated strong support for Internet Anonymity." Electronic Privacy Information Centre, http://epic.org/privacy/survey/.
[33] See *Information Privacy Act 2000 (Vic)* Sch 1 IPP 1 and *Privacy Act 1988 (Cth)* Sch 3 NPP 1.
[34] Marilyn Prosch, 'Preventing identity theft throughout the data life cycle', (2009) *Journal of Accountancy*, accessed at <http://www.journalofaccountancy.com/Issues/2009/Jan/PreventingIdentityTheft.htm>.
[35] Surveys have found Australians regularly do not fill in forms entirely if they believe their personal information is not required, see: Office of the Privacy Commissioner, *Community Attitudes towards Privacy* (2004) <http://www.privacy.gov.au/publications/rcommunity/index.html>.
[36] Such as the sale of informational databases, a 'large industry in the United States', see Ilene Berson & Michael Berson, 'Children and their digital dossiers: lessons in privacy rights in the digital age', (2006) 21 *International Journal of Social Education* 135.
[37] For an in-depth discussion of how the data can be managed over its life-cycle, see: Prosch, above n 34.
[38] Daniel Solove, 'The new vulnerability: data security and personal information', (Working Paper No. 102, Public Law and Legal Theory, George Washington University, 2009), p 2.
[39] Ibid, p 5.
[40] For example, a corrupt employee of a company disclosed 30,000 credit reports, Ibid p 6.
[41] Stephen Mihm, 'Dumpster-Diving for your Identity', *New York Times,* 21 December 2003.
[42] Solove, above n 38, p 7.
[43] See Australian Government Department of Defence, *Information and Communications Technology Security Manual,* (2008) accessed at http://www.dsd.gov.au/library/infosec/ism.html
[44] For example, ISO 27001 provides standards for the management and protection of assets.
[45] For example, in 2006, the US Department of Veteran's Affairs reported the loss of a computer containing the 'name, date of birth, social security number, address and insurance-claim related information' of approximately 16,000 individuals. See Department of Veterans' Affairs, *Latest information on Veterans Affairs Data Security,* (2009) < http://www.usa.gov/veteransinfo.shtml> at 16 June 2009.
[46] For more information regarding encryption, Department of Defence, Above n 42, Chapter 7.
[47] Department of Defence, Above n 43, G-1.
[48] ALRC, Above n 17, [12.27].
[49] Office of the Victorian Privacy Commissioner, *Responding to Privacy Breaches* (2008) Guide Edition 1.
[50] Solove, above n 38, p 2.