Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

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

on the

Inquiry into the adequacy of protections for the privacy of Australians online

23 July 2010

The Deputy Privacy Commissioner wishes to acknowledge the work of Scott May and Jason Forte (Policy and Compliance Officers) 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

Introduction

1) The Privacy Commissioner is currently on leave and has delegated all of her powers and functions to me under section 61(1) of the *Information Privacy Act 2000*.

2) Online privacy is a broad concept, encompassing issues of identity fraud and theft, cyber-stalking, cyber-bullying and grooming by sexual predators, all of which are reported as becoming increasingly prevalent,[1] as well as protecting personal information online more generally. Protecting individuals online ultimately involves empowering them to manage their own behaviour and their personal information when engaging in an online environment. Privacy laws can assist this process by regulating the way in which organisations (both government and private) collect, use, store and manage databases of personal information. Educating individuals about how to protect their personal information online and how privacy laws can operate to assist them is therefore of paramount importance.

3) This submission considers various ways in which privacy laws can address privacy risks to Australians online and some ways in which privacy and data protection regulators in Australia and other jurisdictions have responded to these concerns.

Current privacy landscape

Australian privacy laws

4) The *Privacy Act 1998* (Cth) regulates information held by the Commonwealth public sector, as well as most corporations and credit providers.[2] 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.[3]

5) 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.[4] The IPA regulates protection of information privacy, and provides individuals with a complaint mechanism.[5] The requirements in the IPA, known as 'Information Privacy Principles', are similar in substance to the *Privacy Act's* 'National Privacy Principles'.[6] 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

---

[1] See Standing Committee on Communications, '*Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber* Crime' (June 2010), accessible at http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm (accessed 23 June 2010).

[2] But only corporations with over $3m annual turnover, See *Privacy Act 1998* (Cth) s.6D and for credit providers, Part IIIA

[3] See *Privacy Act 1998* (Cth) Sch 2

[4] *Information Privacy Act 2000* (Vic), s.9

[5] See ss.6 and s.25, *Information Privacy Act 2000* (Vic)

[6] E.g. compare *Privacy Act 1988* (Cth) Sch 3 with *Information Privacy Act 2000* (Vic) Sch 1

to privacy.[7] 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 sector organisations. Each jurisdiction maintains separate privacy regulators to oversee compliance with their individual Acts.[8]

6) 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.[9]

Gaps within current framework

7) 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 'small' businesses.

8) The Victorian Law Reform Commission found 'significant' gaps in the protection of privacy in the workplace.[10] Employee records are specifically excluded from the federal *Privacy Act.* [11] Such records, particularly of large corporate employers, contain vast amounts of employee personal information, and such information remains unprotected under privacy legislation.[12]

9) 'Small' businesses, defined as businesses with an annual turnover of less than $3 million, are exempt from the application of the *Privacy Act.*[13] 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.[14]

10) The ALRC has recommended closure of both of the above gaps and the adoption of consistent, uniform privacy regulation.[15]

---

[7] *Charter of Human Rights and Responsibilities Act 2006* (Vic), s.13
[8] *Privacy and Personal Information Protection Act 1998* (NSW), *Information Act* (NT), *Personal Information Protection Act 2004* (Tas), *Information Privacy Act 2009* (Qld)
[9] See Privacy Victoria, *Privacy Regulation across Australia, as 5 November 2009,* available at www.privacy.vic.gov.au/privacy/web.nsf/content/information+sheets
[10] Victorian Law Reform Commission, *Workplace Privacy Final Report*, Report No 159 (2005) [1.25]
[11] However, as the *Information Privacy Act 2000* (Vic) contains no similar exemption, employee records are protected in the Victorian public sector
[12] *Privacy Act 1988* (Cth), s.7B(3)
[13] *Privacy Act 1988* (Cth), s.6D
[14] ALRC, *For Your Information: Australian Privacy Law And Practice*, Report No 108 (2008), Para 39.21
[15] Ibid, Rec 3.1

Importance of privacy laws

11) Adherence to privacy laws reduces the risk and incidence of privacy risks and can protect individuals online by limiting over-collection of personal information by organisations, prohibiting or preventing use or disclosure beyond the primary purpose of collection and promoting aspects such as anonymity and data security.

12) Privacy laws also impose obligations on an organisation to take reasonable steps to inform individuals of:

i) the identity of the organisation that is collecting the information and its contact details;

ii) the individual's ability to access the information;

iii) the purpose for which the information is collected;

iv) to whom the organisation usually discloses the information;

v) any law requiring the information to be collected; and

vi) the main consequences for the individual if the information is not provided.[16]

13) The significant impact of these obligations is not to be underestimated. For instance, if an organisation is transparent about to whom it discloses personal information and what it intends to do with that information, a person may choose not to engage with that organisation. Organisations should consider whether their current collection notices are reasonably easy to understand so that individuals are able to exercise their privacy rights and make informed decisions.

Individuals and statutory or common law cause of action

14) Whilst legislative provisions provide limited protection of privacy within Australia with respect to the public sector and large corporations, individuals acting in their own capacity have no obligations under any Australian privacy legislation.

15) Additionally, there is currently no recognised common law action for breach of privacy in Australia. Other common law actions (defamation, breach of confidence, nuisance and trespass) [17] and some criminal actions (stalking, harassment) may be used to partially protect privacy rights, but the ability of the common law or equity to address such action is limited.[18]

---

[16] *Information Privacy Act 2000* (Vic), Sch 1, IPP 1.3; *Privacy Act 1988* (Cth), Sch 3, NPP 1.3.

[17] 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), paras 55 & 56, available at www.privacy.vic.gov.au/privacy/web.nsf/content/submissions

[18] E.g. in *Giller v Procopets*, [2004] VSC 113, [2008] VSCA 236, where Gillard J of the Victorian Supreme Court held that the plaintiff was not entitled to recover damages for mental distress in relation to a breach of confidence. The decision was overturned on appeal. The Court of Appeal awarded substantial damages for breach of confidence, but the Court declined to make any findings as to the existence of an equitable or common law right to privacy.

16) The ALRC has recommended establishment of a statutory cause of action for breach of privacy.[19] A statutory cause of action would confer privacy obligations on individuals and expand the protection of privacy within Australia.

17) Enhancement and expansion of existing privacy laws, to close exemptions and to ensure more organisations and individuals 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 or negligent disclosure online.

Identity theft and fraud

18) "Identity theft" or "identity fraud" are broad concepts which describe the theft or assumption of a pre-existing identity used to obtain goods, money or some other financial advantage, or to avoid legal obligations.[20]

19) The concept of identity theft also encompasses situations such as where an individual uses another person's identity for harassment or stalking purposes, often known as cyber-bullying. This may occur on social networking sites such as Facebook or MySpace, or via e-mail. As indicated above, Australian privacy legislation does not impose obligations on individuals acting in their own private capacity. Instead, victims of cyber-bullying need to avail themselves of other legal mechanisms.

Anonymity

20) In dealing or interacting with organisations, individuals should be afforded the opportunity to remain anonymous where possible. All Victorian public sector organisations,[21] as well as some private sector organisations,[22] 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.

21) This concept is also included in the Exposure Draft Australian Privacy Principles currently before the Senate Finance and Public Administration Committee.[23]

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

23) Many websites require the disclosure of personal information by the user – for example, where one registers with a social networking site. This may result in the collection of an individual's full name, date of birth, address or associated information: for instance,

---

[19] ALRC, op cit, Rec 74

[20] See Australasian Centre for Policing Research, '*Standardisation of definitions of identity crime terms: a step towards consistency'* (March 2006) No. 145.3.

[21] *Information Privacy Act 2000* (Vic), s.9, Information Privacy Principle (IPP) 8

[22] *Privacy Act 1988* (Cth), s.6C, National Privacy Principle (NPP) 8

[23] Exposure Draft, Australian Privacy Principles (APPs), APP2, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm, last accessed 13 July 2010

Facebook's Terms of Service states that real names and information must be used to establish an account.[24]

24) Conversely, anonymity can also act as a "cloak" for would- be cyber offenders. Accordingly, promotion of anonymity will only be relevant to certain online behaviours and must be undertaken in consideration of other privacy rights.

Over-collection of personal information

25) 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.

Current legislation

26) 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 some private sector organisations, to 'only collect personal information that is necessary for ...functions or activities'.[25]

Practice of over-collection

27) It is common practice for organisations to 'over collect' the personal information of individuals interacting with them. This is particularly the case online. Over-collection leaves organisations open to larger and more damaging consequences when the security of a database is breached.[26] The more comprehensive the personal information collected, the more valuable it will be to those wishing to commit identity theft or fraud.

Use of mandatory fields

28) One common area of over-collection is the use of mandatory fields. This approach is increasingly common in an online environment when organisations (particularly social networking sites) seek to collect information from an individual. Organisational web sites often contain mandatory fields, stating information is required or necessary for a user to be able 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. Some web browsers now also automatically complete data forms for the user.

29) Most problematic is when web sites refuse to allow 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, such an option is unavailable online, effectively forcing users to provide information in order to access a required service. There is also the possibility that

[24] See www.facebook.com/terms.php, last accessed 13 July 2010
[25] *Information Privacy Act 2000* (Vic) Sch 1 IPP 1; *Privacy Act 1988* (Cth) Sch 3 NPP 1.

[26] Marilyn Prosch, 'Preventing Identity Theft throughout the Data Life-Cycle' (2009) *Journal of Accountancy*.

some users, when faced with a mandatory form, will fill the form with false or inaccurate information in order to proceed. This leads to subsequent problems with data quality and accuracy, particularly if this information is disclosed or used for other purposes.

30) 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.

Danger of Over-collection

31) 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.[27] As a result, personal information held by organisations tends to expand over time, becoming increasingly comprehensive.

Data Security

32) 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.[28]

33) Organisations often devote significant time and resources to the prevention of cyber-interception or 'hacking', viewing online security as a purely technological issue.[29] Whilst important, technological actions alone will not suffice.

Organisational and behavioural practices

34) 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.[30] Data security can be compromised through 'relatively low-tech means' including unauthorised employee action.[31] The US Federal Trade Commission has noted 'strong growth' in 'insider threats', such as employees transferring data to identity thieves.[32] Organisations should implement workplace policies that maintain the security

---

[27] 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.

[28] See Prosch, op cit

[29] 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

[30] Ibid, p 5

[31] E.g. a single corrupt employee of a company disclosed 30 000 credit reports; ibid, p 6

[32] Stephen Mihm, 'Dumpster-Diving for Your Identity', *New York Times*, 21 December 2003

of data from collection to disposal, and ensure computer security infrastructure reflects this approach across the entire organisation.[33]

User Access Control

35) 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.[34] A variety of technical options and standards are available for organisations to implement user access control.[35]

Encryption

36) 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.[36] 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.[37]

Audit control and procedures

37) 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'.[38]

Automatic notification of privacy breach/data loss

38) 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.

---

[33] Solove, op cit, p 7
[34] See Australian Government, Department of Defence, Defence Signals Directorate, *Information and Communications Technology Security Manual*, (2008), accessed at www.dsd.gov.au/library/infosec/ism.html, last accessed 13 July 2010
[35] E.g., ISO 27001 provides standards for the management and protection of assets
[36] E.g. In 2006, the US Department of Veterans' 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) www.usa.gov/veteransinfo.shmtl, last accessed 13 July 2010
[37] See Australian Government, Department of Defence, op cit, Chapter 7
[38] Ibid, G-1

39) The ALRC recommended amendment of privacy laws to include breach notification to the Office of the Privacy Commissioner and potential victims.[39] Whilst notification is not required under current privacy legislation, it is good practice for organisations to do so.[40]

Transborder data issues

40) The effectiveness of privacy laws is limited in an online environment. Data is increasingly transmitted and stored globally, despite privacy regulation occurring at a state and national jurisdictional level. When disclosing their personal information, individuals may not appreciate that their information is being sent out of Australia; it may also be unclear where their information is being sent or stored at all. While Australian privacy laws do provide protection for personal information held within Australia, and impose limitations on transfer of personal information outside the jurisdiction,[41] privacy laws in Australia will be less effective, if not unenforceable, where information is transmitted and stored overseas. If a privacy breach occurs outside Australia, individuals may be powerless to seek remedy. Equally, if a jurisdiction has no privacy laws, Australian law is unlikely to assist an individual seeking to protect personal information held overseas.

41) Given the territorial nature of privacy regulation and the trend to transmit and store data across various jurisdictions, privacy regulators must act collaboratively to deal with the challenges. Examples of this have occurred recently with concerns regarding Google and Facebook. Ten privacy commissioners from Canada, the United Kingdom, France, Germany, Italy, Spain, Israel, Ireland, the Netherlands and New Zealand came together in April 2010 to write an open letter to Google regarding privacy concerns,[42] and Google's "accidental" collection of Wi-Fi data from unsecured wireless networks has received considerable attention from data protection and privacy regulators from Australia, Germany, France, Britain, Spain and Italy, as well as the United States' Federal Trade Commission. The Canadian Privacy Commissioner initiated investigations into Facebook's handling of personal information, finding Facebook had "serious privacy gaps", which resulted in Facebook changing its privacy settings so that users have more control over their personal information. [43] Such examples demonstrate the collaborative response that is required to fully address data protection concerns.

---

[39] ALRC, op cit, [12.27]

[40] Office of the Victorian Privacy Commissioner, *Responding to Privacy Breaches* (2008), available at www.privacy.vic.gov.au/privacy/web.nsf/content/guidelines

[41] See, for instance, *Information Privacy Act 2000* (Vic), Sch 1, IPP 9; *Privacy Act 1988* (Cth), Sch 3, NPP 9. Organisations bound by either Act may only transfer personal information about an individual to someone who is outside Victoria (or Australia) if: (a) the organisation reasonably believes the recipient is subject to a law or contract which effectively upholds principles for the fair handling of the information that are substantially similar to the Information Privacy Principles; (b) the individual consents; (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or between the organisation and a third party to the interest of the individual; or (d) the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual and if it were practicable, the individual was likely to give that consent.

[42] Available from www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf (accessed 23 June 2010).

[43] See Office of the Privacy Commissioner of Canada, http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.cfm (accessed 23 June 2010 and http://www.priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm

42) The ALRC has suggested that, whilst efforts should be made to harmonise transborder data flow laws, the basic principle should be that an agency or organisation that transfers personal information outside the country remains accountable for it, except in specified circumstances.[44] This concept has also been incorporated into the Exposure Draft *Australian Privacy Principles*.[45]

43) All of these issues go to highlight that online privacy issues – particularly ones which involve data transmitted overseas – cannot be addressed by legislative protection alone, but instead require a collaborative effort and approach between different jurisdictions and regulators.

Supporting individuals to help themselves

44) This submission considers that adherence to privacy principles will provide a method of reducing online privacy risks. This is of vital importance as individuals continue to interact online, including social networking sites such as Facebook and MySpace. While adherence to privacy principles and legislative or regulatory reform may be of some assistance, one of the most effective and empowering tool to address online privacy issues is education.

Education is the key

45) Simply put, no regulatory option or legislative measure will be able to be a single panacea to address the myriad of issues in this area. Ensuring that individuals are fully informed and able to understand both the benefits and risks inherent in online interaction and engagement will be, by far, the most effective and efficient method, whether they are engaging in social networking services or transacting online.

46) This is a viewpoint strongly endorsed at Privacy Victoria's '*Watch This Space:* Children, Young People and Privacy' conference held in May 2010. Academics and presenters at the conference considered that while 'sinister...agendas cannot always be avoided, coping strategies must be developed' and that the most effective strategy, education, 'is more likely to result in informed and sensible choices'.[46] Academic commentators reiterated this view, stating that:

> Some degree of risk-taking is inevitable and no software solution or no network management law will make all the dangers go away. If you want total freedom from online danger the only way to ensure that safety is to go offline...overall it might be

(accessed 23 June 2010). The full report of the OPC Canada is available here: http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm (accessed 23 June 2010).

[44] ALRC Report, above n 4, 1063-1129.
[45] Exposure Draft, Australian Privacy Principles (APPs), APP 8, Clause 20 www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm, last accessed 13 July 2010
[46] Candice Jansz, 'Growing up Networked', Paper presented at '*Watch This Space*: Children, young people and privacy conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

better to build relationships and resilience rather than build firewalls and the bankrolls of surveillance service providers.[47]

47) Part of informing individuals of the risks and issues is to allow them to participate in developing their own material and understanding. At the *Watch This Space* Conference, keynote speaker Robyn Treyvaud presented a film regarding the recent phenomenon of 'sexting' – the creating, sharing and forwarding of sexually explicit images and text by teens.[48] The film was produced by a local filmmaker and 40 Bendigo teenagers, aiming 'to inform and to be informed by the community, so that it feels confident enough to deal with cyber issues and work as a community to develop a culture of ethical digital citizenship.' Similarly, the Office of the Privacy Commissioner of New Zealand's Youth Advisory Group has produced material specifically encouraging young people to think about how their personal information is managed.[49]

48) Other presenters at the Conference highlighted that some jurisdictions have begun to introduce Information and Communications Technology training and education as soon as early childhood.[50] The challenge for educators will be ensuring such educational programmes meet the needs of young people, and ensure they are developed by 'talking with young people, not to them'.[51]

Conclusion

49) 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 is maintained from collection to disposal.

50) Whilst proportional technical measures to mitigate e-security risks are to be encouraged and applauded, such measures alone will be insufficient.

---

[47] Bruce Arnold, 'Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies, Paper presented at '*Watch This Space*: Children, young people and privacy conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

[48] See Robyn Treyvaud, 'Children and Young People, Living Very Public-Private Lives Online', paper presented at '*Watch This Space*: Children, Young People and Privacy Conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

[49] See http://www.privacy.org.nz/youth.

[50] Liz Butterfield, 'Privacy, Digital Citizenship and Young Children', Paper presented at '*Watch This Space*: Children, young people and privacy conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

[51] Robyn Treyvaud, 'Children and Young People living very public-private lives online', Paper presented at '*Watch This Space*: Children, young people and privacy conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

"Even a fortress with impenetrable walls is hardly secure if the back gate is left open".[52]

DR ANTHONY BENDALL
Deputy Victorian Privacy Commissioner

[52] Solove, op cit, p 2