Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Joint Select Committee

on

Cyber-Safety Issues Affecting Children and Young People

25 June 2010

The 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

1. Introduction

1. Cyber-safety is a wide concept, encompassing issues of identity 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 young people online is ultimately about how they 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 children about how to protect their personal information online and how privacy laws can operate to assist them is therefore of paramount importance.

2. This submission considers various ways in which privacy laws can address cyber-safety concerns amongst young people and how privacy and data protection regulators in Australia and other jurisdictions have responded to these concerns.

2. Current privacy landscape

Privacy laws in Australia

3. Protection offered by privacy legislation applies equally to young people and adults.[2] Adherence to privacy laws reduces the risk and incidence of cyber-safety issues relating to young people, and can protect young people 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.

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

    (a) the identity of the organisation that is collecting the information and its contact details;
    (b) the individual's ability to access the information;
    (c) the purpose for which the information is collected;
    (d) to whom the organisation usually discloses the information;
    (e) any law requiring the information to be collected; and
    (f) the main consequences for the individual if the information is not provided.[3]

5. The significant impact these obligations have on an organisation is not to be underestimated. For instance, if an organisation is transparent about to whom it discloses

[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] Such as the *Information Privacy Act 2000* (Vic) and the *Privacy Act 1988* (Cth).

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

personal information and what it intends to do with that information, a young person may choose not to engage with that particular online site. For organisations interacting and collecting directly from children, organisations should consider whether their current collection notices are reasonably easy to understand so that children are able to exercise their privacy rights and make informed decisions.

Individual action and statutory action for breach of privacy

6. Australian privacy legislation does not impose any obligations on individuals acting in a private capacity; rather, the legislation relates to how organisations deal with personal information. There are significant exceptions: for example, businesses with a turnover of less than three million dollars are not subject to any privacy legislation.[4]

7. As such, privacy legislation may not be sufficient to protect children from cyber-safety risks that occur as a result of individuals acting in a private capacity. Other common law actions (defamation, breach of confidence, nuisance and trespass), and some criminal actions (stalking, harassment), may be used to partially give privacy rights where an individual is involved, but the ability of the common law to address such action is limited.[5]

8. The Australian Law Reform Commission (**ALRC**) has recommended establishment of a statutory cause of action for breach of privacy.[6] A statutory cause of action would confer privacy obligations on individuals. I have previously acknowledged that establishing a statutory cause of action for breach of privacy would expand the protection of privacy within Australia.[7] 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 cyber-crime (for example, identity fraud and theft) to be committed against young persons.

Identity theft

9. "Identity theft" is a broad concept which describes the theft or assumption of a pre-existing identity used to obtain goods, money or some other financial advantage, or to avoid legal obligations.[8] With the rise of online social networking sites and instant messaging programs, additional issues related to identity theft such as impersonation and the use of fake accounts for cyber-bullying purposes are becoming increasingly prevalent.

---

[4] *Privacy Act 1988* (Cth), Sch 3, NPP 6C, 6D.

[5] For example, in *Giller v Procopets* [2004] VSC 113, where Gillard J 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 damages for breach of confidence, but the Court declined to make any findings on whether or not there had been a breach of privacy.

[6] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 3.1.

[7] Submission of the Victorian Privacy Commissioner to the House of Representatives Standing Committee on Communications on its Inquiry Into Cyber Crime, July 2009.

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

10. 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

11. Recent studies have suggested that young people tend to participate in online behaviour involving disclosure of significant amounts personal data (for example, social networking); however, young people still maintain an aspiration for privacy to the same degree as adults.[9] Accordingly, in dealing or interacting with organisations, individuals (including children) should be afforded the opportunity to remain anonymous where possible. All Victorian public sector organisations, as well as some private sector organisations, 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.[10] The option of not identifying oneself restricts the personal information that is communicated to, and retained by, the organisation. Less information is then available to would-be cyber criminals in the event of a data breach.

12. Many websites 'require' the disclosure of personal information by the user – for example, where a young person registers with a social networking website. This may result in the collection of a child's full name, address or associated information: for instance, Facebook's Terms of Service states that real names and information must be used to register an account.[11] Young persons may also be more likely to reveal personal information about themselves to receive a reward or discount – such as is required when signing up for an online game or contest.[12]

13. On certain sites such as instant messaging or chat rooms, children may also assume that using the Internet is anonymous and therefore appears 'safe'. This may increase the likelihood of a young person sharing their own personal information with someone they otherwise would not.

14. It is worth noting however that anonymity can also act as a "cloak" for would-be cyber-offenders. Accordingly, promotion of anonymity may only be relevant to certain online behaviours and must be undertaken in consideration with other privacy rights.

---

[9] Chris Jay Hoofnagle, Jennifer King, Su Li, Joseph Turow, '*How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*' (April 14, 2010). Available at SSRN: http://ssrn.com/abstract=1589864. Note, however, that this paper studied young adults in America between the ages of 18-24, rather than young persons under the age of 18.

[10] *Information Privacy Act 2000* (Vic), Sch 1, IPP 8.1; *Privacy Act 1988* (Cth), Sch 3, NPP 8.

11 See http://www.facebook.com/terms.php (accessed 23 June 2010).

[12] Report of the Child Health Promotion Research Centre, *Review of Existing Australian and International Cyber-Safety Research*, May 2009.

Over-collection of personal information

15. 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

16. 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 its functions or activities'.[13]

(b) Practice of over-collection

17. 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.[14] The more comprehensive the personal information collected, the more valuable it will be to those wishing to commit identity theft or fraud.

(c) Use of mandatory fields

18. 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.

19. 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 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.

20. 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.

---

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

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

(d) Danger of Over-collection

21. 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.[15] As a result, personal information held by organisations tends to expand over time, becoming increasingly comprehensive.

Data security

22. The more data an organisation collects, the more secure it has to keep it.[16] Organisations should take adequate steps to prevent loss or unauthorised disclosure of personal information that is necessary to collect. Accordingly, where an organisation over-collects information, it increases the risk of misuse, unauthorised access or disclosure.

23. It is usual for organisations to hold personal information of children, either as customers or clients. It is therefore important that an organisation takes reasonable steps to keep secure data that it holds under the relevant privacy legislation. This can be achieved in a variety of ways, including restricting access controls on personal information databases within organisations, encryption and conducting proactive audit control on databases.[17]

3. Transborder data issues

24. The effectiveness of privacy laws are 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, children 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,[18] 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,

---

[15] 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.

[16] *Information Privacy Act 2000* (Vic), Sch 1, IPP 4.1; *Privacy Act 1988* (Cth), Sch 3, NPP 4.1.

[17] See Submission of the Victorian Privacy Commissioner to the House of Representatives Standing Committee on Communications on its Inquiry Into Cyber Crime, July 2009, available at http://www.privacy.vic.gov.au.

[18] 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.

Australian law is unlikely to assist an individual seeking to protect personal information held overseas.

25. 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,[19] 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.[20] Such examples demonstrate the collaborative response that is required to fully address data protection concerns.

26. 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.[21]

27. All of these issues go to highlight that cyber-safety 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.

4. Supporting young people to protect themselves

28. This submission considers that adherence to privacy principles will provide a method of reducing the risk and incidence of cyber-safety issues relating to young people. This is of vital importance as children 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, I consider one of the most effective and empowering tool to address cyber-safety issues amongst young people is education.

Education is the key

29. 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 young people are fully

---

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

[20] 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 (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).

[21] ALRC Report, above n 4, 1063-1129.

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 young people are engaging in social networking services or transacting online.

30. This is a viewpoint strongly endorsed at Privacy Victoria's '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'.[22] 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 better to build relationships and resilience rather than build firewalls and the bankrolls of surveillance service providers.[23]

31. Part of informing children of the risks and issues is to allow them to participate in developing their own material and understanding. At the 'Children, Young People and Privacy' 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.[24] 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.[25]

32. 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.[26] 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'.[27]

---

[22] Candice Jansz, 'Growing up Networked', Paper presented at the 'Children, young people and privacy conference', Melbourne, 21 May 2010 (available at http://www.privacy.gov.au).

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

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

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

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

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

Technical constraints alone will be insufficient

33. There is a significant danger of going 'too far down the road' in implementing technical constraints on online environments. If ultimately disproportionate controls on internet usage are introduced (either for children specifically, or all citizens in general), society risks trading off some of the benefits of online interaction and offering only a sanitised and controlled version of interaction. I seriously question whether the ISP internet filtering proposal of 'refused classification' level at a national level represents a proportional response to concerns raised.

34. Additionally, the effectiveness of filtering as a means of protecting children online has been seriously questioned. Filtering 'may not be an effective strategy' and significant 'limitations (are) associated with filtering technology'.[28]

35. A comprehensive educative programme, which begins when children first begin to interact with online environments and continuing through to the different challenges of late adolescence, is required and supported. Technical constraints have a place, but it should not be the predominant one.

5. Conclusion

36. There is no singular solution to ensuring the protection of young people online. Privacy laws can assist by regulating the way in which organisations collect and deal with personal information, but ultimately, educating young people of the implications of releasing their personal information is the best method to achieving a safer online environment.

HELEN VERSEY
Victorian Privacy Commissioner

[28] Dooley, JJ, Cross, D, Hearn, L, Treyvaud, R. 'Review of existing Australian and international cyber-safety research', Child Heath Promotion Research Centre, Edith Cowan University, Perth (p. 178-183), accessible at http://www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf.