SUBMISSION No. 92

Australian Government

Office of the Privacy Commissioner

Inquiry into Cyber Safety Issues Affecting Children and Young People

Submission to the Joint Select Committee on Cyber Safety

July 2010

Key recommendations

The Office of the Privacy Commissioner (the Office) welcomes the opportunity to provide comments to the Joint Select Committee on Cyber Safety about cyber safety issues affecting children and young people.

We believe privacy awareness is an important element of improving cyber safety for children and young people. The proliferation of online activities and associated privacy risks, coupled with the fact that young users are often less aware of the risks, suggests that there is a particular need for educational activities aimed at raising privacy awareness amongst children and young people.

The Office's main suggestions for improving cyber safety for children and young people are:

1. Education is the key to empowering individuals to protect their privacy online and, more broadly, to establishing good cyber safety behaviours. This is especially important for more vulnerable individuals such as children and young people.

2. Our Office would generally be supportive and welcome involvement in future educational activities.

3. Cyber safety is a national problem and requires a coordinated approach across portfolios and jurisdictions. Ensuring that various education and awareness programs are complementary and co-ordinated is important to promoting a cyber safe community.

4. The Office supports Australia's continuing involvement in initiatives of international forums.

5. The Office considers that privacy should be treated as a separate topic within broader cyber safety education activities and not bundled with other concepts.

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (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.

The Privacy Act

2. The Privacy Act generally covers the protection of people's personal information. 'Personal information' 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. Under the Privacy Act, personal information can exist in a number of different forms, including in images such as photographs.

3. The Privacy Act is also intended to be principle based and technology neutral. What this means is that the Privacy Act does set out prescriptive rules about how information should be handled in particular situations, such as online environments. Instead it offers principles about the way in which personal information should be handled according to the particular situation.

About this submission

4. The Office of the Privacy Commissioner (the Office) welcomes the opportunity to comment on the Australian Parliament's Joint Select Committee inquiry into the safety of children and young people on the internet.

5. The Office notes the terms of reference that have been provided for this review of cyber safety.[1] Cyber safety is a broad concept that concerns minimising the risks to children online from a range of negative influences including inappropriate social behaviours, abuse, identity theft and breaches of privacy. These negative cyber incidents can potentially have broader long term effects for both children and their families.

[1] The terms of reference for this inquiry are available at: http://www.aph.gov.au/house/committee/jscc/tor.htm (as at 1 June 2010)

6. As cyber activity very often involves personal information there is a strong connection between privacy and cyber safety issues. Personal information is increasingly becoming digitised and transmitted online increasing the risk of privacy breaches and identity theft. Privacy and security of personal information in online environments are therefore important elements of cyber safety.

7. The Office considers that educating young people about privacy could assist in improving cyber safety outcomes. Our submission focuses on issues related to privacy as an important component of cyber safety. Throughout this submission the Office provides examples of cyber safety initiatives currently in place and comments on future initiatives.

8. This submission draws on previous comments we have made about the important role privacy protections can play in minimising risks online including our comments to the Australian Law Reform Commission's (ALRC) review of privacy law in Australia.[2]

Children and young people's privacy

9. Children are particularly vulnerable due to their limited capacity to make decisions about their own information and their reliance on others to ensure that their interests and rights are protected. The potential consequences on a child or young person of a breach of their privacy rights at this developmental stage of their lives include the risk of trauma, embarrassment or stigmatisation and even the possibility of identity theft.

10. The Privacy Act does not currently make special reference to children and young people, and instead operates on the basis that children and young people have the same rights to privacy as adults. In practice however, a child's primary care giver will usually be responsible for exercising the child's rights under the Privacy Act until the child reaches a level of maturity and understanding to make independent decisions.

11. The Office considers that this approach to the privacy of young people is appropriate, as it accommodates different rates of development. Mature young people are entitled wherever possible, to make decisions about their personal information as soon as they are able, rather than on reaching a prescribed age. It is the Office's view that this level of autonomy should be maintained in respect of young people's privacy.

[2]ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (http://www.austlii.edu.au/au/other/alrc/publications/reports/108/)

Level of understanding

12. There has been little Australian research on the awareness or attitudes of children and young people to privacy issues. However, initiatives such as recent conference in Victoria[3] and the work of the New Zealand Youth Advisory Group[4] have sought to gain further insight into what privacy means to children and young people today and how it affects them. In particular, the conference hosted by Privacy Victoria also considered the potential risks associated with the use of information technologies and what educators, policy makers, parents and even young people themselves can do to educate young people about privacy protection.

13. The available evidence suggests that more effort needs to be directed to ensuring young people gain the skills needed to make sensible decisions around privacy and to understand their rights and obligations under the Privacy Act.

14. Results from the Office's 2007 Community Attitudes Survey[5] suggested that while awareness of privacy issues has increased overall in comparison to 2004, younger respondents (in this case, aged 18-24) continue to be less aware of their privacy rights than older respondents. This may correspond with levels of awareness of legal rights more generally. The survey also showed that 50% of respondents were more concerned about providing information over the internet than they were two years earlier. However, a higher proportion of respondents aged 18-24 claimed to be less concerned than other age groups.

15. The survey also indicated that young people were less concerned about disclosing their financial information and are much more likely to disclose their personal information in order to receive a discount or to win a prize. These types of behaviours, and being less informed about privacy issues could put young people at risk of identity theft. Another recent survey by Galaxy Research[6] has also shown that young people (in this case, aged 18-24) were most at risk of identity fraud and were more complacent about checking for enhanced security features before providing sensitive information online.

---

[3] See http://www.privacy.vic.gov.au/privacy/web.nsf/content/conferences

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

[5] Wallis Consulting Group, *Community Attitudes Towards Privacy 2007 [prepared for the Office of the Privacy Commissioner]* (2007) available at http://www.privacy.gov.au/publications/rcommunity07.pdf

[6] *VeriSign Online Fraud Barometer*, compiled by Galaxy Research as at 6 July 2010 available at http://www.verisign.com.au/press/2010/20100706.html

16. The Office believes that identity theft constitutes a serious interference with individuals' privacy and is becoming an increasingly important issue. Identity theft occurs where an individual obtains personal information (e.g. credit card, drivers licence, passport or other personal identification documents) and uses that information to fraudulently obtain a benefit or service for themselves. Whilst identity theft is often associated with the financial loss of adults, identity theft can also have serious consequences for young people when their identity is stolen for the purposes of fabricating fake documents such as passports or to commit further cyber crime.

17. Based on the available evidence, it is our view that young users are at risk of inadvertently becoming victims of cyber incidents as a result of inadequate cyber safety skills. The proliferation of online activities and associated privacy risks, coupled with the fact that young users are less aware of the risks, suggests that there is a particular need for educational activities aimed at raising privacy awareness among this group. Such measures will assist in building a sound foundation for children and young people to make informed decisions about protecting their own privacy and respecting the privacy of others.

End user empowerment

18. The Office believes education is the key to empowering individuals to protect their privacy online. We consider this also extends to cyber safety. People of all ages need to be equipped with the necessary cyber safety skills to safely navigate the online environment. The Privacy Commissioner has a statutory function to promote the protection of individual's privacy by undertaking educational programs either solely or in co-operation with other parties.[7]

19. 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.[8] Much of this advice for individuals is provided in a series of 'frequently asked questions' and is designed to be easily accessible.

20. In the Office's view, a range of measures are required to empower individuals to protect themselves in online environments and are essential to promoting effective privacy and cyber safety. These measures can include promoting education and awareness of the:

[7] See section 27(1)(m) of the Privacy Act

[8] For more information see following links to the Office's website in regards to: FAQs on social networking http://www.privacy.gov.au/faq/individuals#social_networking, Online Privacy Tools http://www.privacy.gov.au/topics/technologies/security, and Protecting your privacy on the internet http://www.privacy.gov.au/topics/technologies/privacy

- risks posed by various ICT environments and interactions
- measures that can be taken to mitigate risk, whether through technology or individual behaviour
- remedies available should something go wrong

21. Children and young people can potentially be exposed to the same range of risks online as older people but may be more vulnerable to online risks. Recognising this, the Office has created some materials targeted specifically towards young people.

22. In particular, we have developed a Youth Portal, released during Privacy Awareness Week 2009 which allows young people to learn about current privacy issues. The portal includes *Private i- Your Ultimate Privacy Survival Guide* and a short animated video, *Think Before You Upload* (a joint initiative of the Asia Pacific Privacy Authorities).

23. 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.[9] Further, they seek to build awareness of the Office and its website as a resource for young people, including material that sets out their privacy rights and how to exercise them[10]. In our view, whils*t* regulatory approaches can help to control inappropriate online behaviours, legislative mechanisms are not always an effective response to regulating online risks. We consider that education is key to helping children and young people gain lifelong cyber safety skills and develop respect for privacy. Our Office would generally be supportive and would welcome involvement in any future educational activities.

Cross-jurisdictional co-operation

24. Cyber safety is a national problem and an important way to minimise cyber safety risks is to adopt a coordinated approach across portfolios and jurisdictions. 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 responses. Ensuring that various education and awareness programs are complementary and co-ordinated is key to promoting an empowered community.

[9] See http://www.privacyawarenessweek.org/topics/youth/index.html

[10] See http://www.privacy.gov.au/privacy_rights/complaints/index.html

25. As part of this year's Privacy Awareness Week, the Office partnered with Department of Broadband, Communications and the Digital Economy (DBCDE), as well as the Australian Communications and Media Authority, to promote key messages that are of common concern. In particular, to encourage Australians to think about privacy and cyber security when using mobile phones a pocket-sized quick reference guide titled *Mobilise Your Mobile Phone Privacy*[11] was produced. The guide gives mobile users ten simple, easy to understand tips for protecting their privacy and security when using their mobile phones.

26. In our view, a range of initiatives and channels are required to ensure an effective response to cyber safety issues. For this reason, the Office has been supportive of the cyber safety and e-security activities undertaken by Government agencies. For example, the e-security education and training materials developed by the DBCDE,[12] as well work done by NetAlert,[13] and resources such as www.staysmartonline.gov.au and www.cybersmartkids.com.au (provided by the Australian Communications and Media Association). A further example is the National Cyber Security Awareness Week, an initiative of DBCDE's 'Stay Smart Online' program. This event is a collaborative effort between government, industry and community groups, which urges both organisations and individuals to be aware of e-security risks and how to interact securely online.[14]

27. The Office believes that there is also a need to ensure a consistent and collaborative approach to cyber safety across different levels of government. In our view, appropriate forums for such initiatives could be inter-jurisdictional forums, such as the Privacy Authorities Australia (PAA) forum. 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 and discusses on co-ordinated approaches to issues affecting individuals' personal information.

28. 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.

---

[11] Copies of the pocket guide are available from the Office of the Privacy Commissioner

[12] More information on this initiative is available at http://www.dbcde.gov.au/communications_for_consumers/security/e-security

[13] See http://www.netalert.gov.au/

[14] See http://www.privacy.gov.au/materials/a-z?fullsummary=7090

29. The Office supports achieving national uniformity in privacy regulation, as recommended by the ALRC in its review of privacy law and supported by the Australian Government in its first stage response.[15] The Office considers that greater consistency in privacy regulation would enhance security for information flowing across State and Territory boundaries which in turn can aid improved cyber safety outcomes.

International co-operation

30. In the Office's view, an important component to promoting effective online privacy and cyber safety is to recognise the international cross-jurisdictional nature of many modern information flows. In turn, this requires international co-operation to foster good privacy outcomes and the promotion of cyber safety.

31. Forums such as the Asia Pacific Privacy Authorities, the Organisation for Economic Cooperation and Development Working Party of Information Security and Privacy (WPISP) and work done by Asia Pacific Economic Cooperation (APEC) economies on developing an APEC privacy framework all provide tangible examples of how such an objective can be progressed.

32. The Office supports Australia's continuing involvement in the privacy initiatives of the following international fora.

33. WPISP develops policy options to encourage privacy protection in a networked society.[16] Some of WPISP's work has included looking at the future of the internet economy from a privacy and security perspective and policy approaches for the protection of children online. The Office continues to provide input into the work of WPISP.

34. APEC has a number of initiatives aimed at protecting information privacy and maintaining information flows among APEC economies. A key initiative is the *APEC Privacy Framework*, agreed in 2004. The Privacy Framework contains nine high level Privacy Principles that represent a minimum standard. The Privacy Frame work aims to promote a consistent approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.

35. The Office is a member of the Asia Pacific Privacy Authorities (APPA) forum.

---

[15] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 3-4, recommendation 3-5, recommendation 3-6

[16] For information on OECD WPISP, see www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html

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.[17] 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.

36. APPA members have undertaken a number of joint initiatives such as Privacy Awareness Week to promote awareness of privacy rights and responsibilities. Specifically for young people, a short animated video and accompanying teacher resources warning of the dangers of social networking websites was released by APPA members in May 2009.

37. APPA members also developed an online self help identity theft prevention tool for Privacy Awareness Week 2010.[18] It is an interactive quiz-based tool which helps individuals to work out how likely they are to be a victim of identity theft. The tool also includes separate 'read and learn' pages with practical tips and ways to improve identity security.

38. Whilst not specifically aimed at young people, the tool considers situations that are also applicable to young people particularly as they gain greater financial and social independence. For example, young people need to aware of the risks of identity theft associated with wallets, driver's licences, online shopping, mobile phones and personal computers.

Future initiatives

39. The ALRC in its review of privacy recommended that the Office, in consultation with ACMA, should ensure that specific guidance on the privacy aspects of using social networking sites is developed and incorporated into publicly available education material.[19] 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.[20]

40. 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

[17] See http://www.privacy.gov.au/aboutus/international/appa

[18] Available at http://www.privacyawarenessweek.org

[19] ALRC, *For Your Information: Australian Privacy Law and Practice*, recommendation 67-3

[20] Ibid, recommendation 67-4

and educational needs facing young people.

41. The Office considers that privacy should be treated as a separate topic within broader cyber safety education modules and not bundled with other concepts. Education activities should help children to start thinking about themselves as individuals with an identity that is linked to their personal information such as their name, address, telephone number, birth date and school. Children should be made aware of the reasons why they need to protect their personal information, and that of others, especially online, along with practical steps they can take to protect their privacy. Education activities should also include advice about how, where and when to get help if they are unsure about providing or protecting their personal information online.

42. The Office notes that education and awareness programs for privacy and online safety should take into account the increasing ubiquity of ICT in many day to day transactions. The use of mobile phones to connect to the internet and facilitate online services is ever increasing along with the increased use and dependence on mobile phones by children and young people. Young users need to be aware of how to protect their privacy when using mobile phones. This is particularly important as mobile phones can store large amounts of personal information and are easily lost or stolen. The Office has recently partnered with other Government agencies to raise community awareness about privacy and security when using mobile phones.[21]

[21] *Mobilise Your Mobile Phone Privacy* a pocket-sized quick reference guide available from the Office of the Privacy Commissioner