

submission

Submission by Privacy NSW to

***Australian Government Joint Select
Committee on Cyber-Safety***



privacynsw

Issue date:

25 JUN 2010

Senator Dana Wortley
Committee Chair
Joint Select Committee on Cyber-Safety
PO Box 6021
CANBERRA ACT 2600

Enquiries: Siobhan Jenner
Tel: (02) 80191603
Our ref: A10/0830
Your ref:

Attn: Jerome Brown
A/g Committee Secretary
jscc@aph.gov.au

Dear Senator

Re: Privacy NSW Submission on cyber-safety issues affecting children and young people

Privacy NSW is pleased to be able to make this submission to the Australian Government's Joint Select Committee on Cyber-Safety regarding the safety of children in an on-line environment.

Privacy NSW is the Office of the NSW Privacy Commissioner. The Privacy Commissioner is the holder of an independent statutory office, created by Parliament under the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The functions of the Privacy Commissioner include making public statements about matters relating to the privacy of individuals generally, and publishing reports and making recommendations about any matter that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals.

This submission reviews the NSW privacy regulatory framework, discusses the broad issue of the expectation of privacy in cyber-space, the issue of consent in the context of children and young people and briefly looks at the issue of identity theft. In making this submission we are cogniscent of the current legislative review of NSW and Commonwealth privacy laws possibly resulting in changes to the legal framework governing the protection of personal and health information in Australia and which may therefore impact upon any proposed regulation of access to or protection from on-line services.

Privacy in Cyberspace

In considering cyber-safety issues as they affect children and young people, we first need to consider how we characterise the concept of privacy in the landscape of the internet.

The PPIP Act, the *Health Records & Information Privacy Act* (HRIP Act) and in *Privacy Act 1988* (Cth) provide a principle-based approach for dealings with personal and health information respectively and mechanisms for dealing with breaches of those principles. None of those laws regulate the actions of individuals acting in their private capacity. In the case of the PPIP Act only dealings with personal information by NSW public sector agencies are subject to limitation. Importantly, there is no



privacynsw

definition of privacy in the PPIP Act, the HRIP Act or in the Privacy Act. Privacy is sometimes defined as a protective concept, made apparent by the impact of its absence:

Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can be easily confused with knowledge.¹

A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.²

Given lack of universal definition as to what constitutes privacy and in light of the limits of privacy laws, how can we describe and then deal with the covert or overt collection, or the publication of personal information which constitute a threat to our sense of freedom or which results in misjudgement about ourselves?

The NSW Law Reform Commission recently considered the concept of privacy in its report on the possible introduction of statutory cause of action for breach of privacy³. That report concludes that the key element of a statutory cause of action for a breach of privacy is that of a 'reasonable expectation of privacy'⁴. So, when we enter cyber-space is our expectation of privacy reasonable or unreasonable? The answer to this depends very much not only as to whether there is an applicable privacy law, on our intentions, on the security of our computer software or the security and veracity of the sites we visit, but also on our capacity understand the risks and to agree to the collection, use and/or publication of our personal information. This issue is dealt with below in the context of children and young people.

As we reported to the Australian Law Reform Commission on its *Discussion Paper 72: Review of Australian Privacy Law* individuals who have made complaints to Privacy NSW often express feelings of powerlessness when they become aware that their image or information about them has been posted on the internet without their consent⁵. Where information about the individual untrue or is embarrassing individuals experience a more acute sense of invasion; a feeling exacerbated by the knowledge that the internet is a forum of potentially unlimited publicity.⁶

Despite such risks, individuals continue to engage with and divulge information into cyber-space. Why? Because despite the risks, we want what is in the box and we expect, if somewhat naively, that our privacy will not be violated when we enter cyber-space. Even where there are safeguards against the misuse of personal

¹ Jeffrey Rosen, *The Unwanted Gaze*, Random House, New York 2000

² Zelman Cowen, 1969, 'The Private Man', *The Boyer Lectures*, Australian Broadcasting Commission, pp 9-10.

³ http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_cp01toc

⁴ NSW Law Reform Commission:

http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_r120report#R1 at 1.1.

⁵ As an example see Privacy NSW's *Annual Report 2005-06* at p31. This case highlighted the difficulties associated with removing personal information published on a website.

⁶

http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications#16, at p10



information such as filters are we engaging them? The *Sydney Morning Herald* recently reported, less than half the parents surveyed by Norton in its Online Family report 2010 have 'activated software filters and control features at home'⁷ when their children use the internet. To expect our personal information to be protected in an environment which is notoriously unsafe⁸ without taking steps to minimize the risk of misuse of that information is unwise could render an expectation of privacy unrealistic, however subsequent misuse of that information for illegal or harmful purposes raises the spectre not only of a breach of a reasonable expectation of privacy but moral and criminal culpability.

The following sections ask firstly, whether it is possible or should be possible for children or young people to consent to the collection, use and/or publication of their personal information in cyber-space and secondly, whether their activities in cyber-space should be monitored and/or limited by parent's guardians or carers.

Consent of children and young people in cyber-space

Whether an individual's expectation of privacy on the internet is reasonable will also be affected by any on-line agreement they may have entered into or the degree of detail of their personal information they have provided. This is further affected by the capacity of that individual to agree/consent to the potential use of their personal information. In the case of internet sites which require an agreement to participate (excluding contractual matters), such as social networking sites, the question is therefore whether a child or young person has the capacity in the circumstances to consent to that use.

On the issue of consent in the context of NSW privacy laws we advise NSW public sector agencies and organizations which hold health information, to assess the whether children and young people with whom they have dealings have the capacity to provide their consent to dealings with their personal information. We further advise that the capacity to consent should be measured on a sliding scale of factors, such as age, the ability to communicate consent, the individual's understanding of the issue in question, support from parents or other authorised representatives and the context in which the issues arise.

Using this model in the context of the safety of children and young people using internet, the question is therefore whether a child or young person can have a reasonable expectation of privacy, given the unfixed nature of the capacity to consent and given that internet is notoriously insecure and that children and young people do not always appreciate the harm that can arise from the misuse of their personal information. In our view the expectation of privacy for the information of children and young people should not necessarily be immediately proxied to parents, guardians or care-givers because this does nothing to alert children and young people to the risks

⁷ <http://www.smh.com.au/digital-life/digital-life-news/our-online-family-portrait-slightly-paranoid-20100616-yf2n.html>. Also see *Watch this Space: Children and privacy conference*, Melbourne, May 2010, Bruce Arnold, at p 16.

⁸ <http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm> at 2.79 to 21.08.



of sharing their information online. Instead we suggest that parents, guardians and care-givers should be encouraged to engage with children and young people to discuss the benefits and risks of providing personal information. In this regard we note the tools available to parents, guardians and carers to assist in this process⁹

Monitoring

In terms of monitoring the activities of children and young people there are obvious privacy implications, from concerned parent the standing over the shoulder of a 10 year old using Facebook, to the use of software to track access a teenagers access to online sites. As one academic notes there are great risks beyond a reasonable expectation of privacy which may be violated by the use of electronic monitoring of children and young people:

A fundamental concern about mooted surveillance technologies is that they embody a mistrust that corrodes personhood and that they are an electronic substitute for the trust (and risk sharing) that we might see as fundamental to family life in 2010.

...the watched are denied full personhood through treatment as data subjects rather than as individuals with personal identity and agency¹⁰

We suggest that parents, guardians and carers be advised to discuss their concern about on-line content with children and young people and that they be encouraged to use the many tools available to do so.¹¹

Identity theft

The use of personal information by a third party to assume the identity of the person to whom the information relates is perhaps the most detrimental risk to the integrity of one's identity and therefore to privacy. The theft of the identity of an individual particularly that of a child or young person can affect personal relationships, financial security, prevent that individual from making life choices and can provide extremely difficult to remedy. We therefore support measures to prevent, prosecute and remedy identity theft as long as they are not at the expense of individual users of the internet.¹²

⁹ See <http://www.cybersmart.gov.au/en/Parents/Risks%20and%20concerns.aspx>. The Office of the Privacy Commissioner also provides very useful information for young people about the on-line risks on its dedicated youth privacy pages: <http://www.privacy.gov.au/topics/youth>

¹⁰ Bruce Arnold, at p17 & p 29.

¹¹ See

<http://www.cybersmart.gov.au/Parents/Risks%20and%20concerns/Inappropriate%20content.aspx>; <http://www.netalert.gov.au/filters.html>

¹² See

<http://www.cybersmart.gov.au/Parents/Keeping%20your%20computer%20secure/Private%20information.aspx> which provides to parents about protecting personal information relating to children.



Conclusion

As we see, it the role of Privacy Commissioners in the protection of children and young people in cyberspace is to assist in balancing the desires of parents, guardians and carers to 'vet the net' on behalf of children and young people¹³ with the need for the free flow of information and the expectation of those children and young people that they will not be constantly surveilled.

Further, Privacy Commissioners have a role in assisting law and policy makers in treading lightly over that expectation where there are significant threats to the health or safety of children and young people or where there is a significant risk that their identity may be stolen. In our view it is this reasonable expectation of privacy which should guide policy and law makers in their consideration of cyber-safety issues affecting children and young people.

Yours sincerely

John McAteer
Principal Privacy Officer
(Delegated **Privacy Commissioner**)

¹³ In his presentation to the *Watch this Space: Children and privacy conference*, Melbourne, May 2010, Bruce Arnold suggests that instead of surveilling the use of the internet by children and young people we should build 'relationships of trust; rather than build ' smart networks' or rely on legislation to avoid cyber-risks. 'Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies, at p 18.

