The adequacy of protections for the privacy of Australians online

To: Senate Standing Committee on Environment and Communications

20 December 2010 (extension granted)

Queries regarding this submission should be directed to:

Contact persons *Alice Palmer*
Ph *(03) 9607 9381*
Email *apalmer@liv.asn.au*

Table of Contents

The Law Institute of Victoria thanks the Committee for the opportunity to have appeared before it on 1 December 2010. The following clarification and responses to questions on notice from the hearing should be read in conjunction with the oral evidence given at the hearing of 1 December 2010 and the written submission to the Committee of 29 July 2010.

Clarification concerning communications with Attorney-General

In response to a question concerning communications with the Attorney-General on the subject of the inquiry, Ms Miller indicated in oral evidence to the Committee on 1 December 2010 that the LIV had written to and received a response from the Attorney-General (p28 of the Proof of Committee Hansard).

Please note that we copied the Attorney-General on our submission to the Committee on 29 July 2010 but did not receive an acknowledgement or response from the Attorney-General. The LIV had, however, written to the Attorney-General in January 2010 in relation to another privacy matter – the Department of Immigration and Citizenship biometric acquisition pilot – to which the LIV was pleased to have received a response. It was this letter to which Ms Miller referred in her evidence.

QoN1 (p26-7) A statutory cause of action for invasions of privacy

The Law Institute of Victoria considers that there should be a statutory cause of action for invasions of privacy.

In our submission to the Victorian Law Reform Commission (VLRC) on the 'Surveillance in Public Places' Consultation Paper,[1] the LIV noted the proactive steps taken in the courts to provide common law protection for privacy.[2] We expressed concern, however, that the evolution of any common law protection will be too slow and too limited to provide appropriate safeguards in the face of new surveillance technologies and other pressures on privacy protection (e.g. counter-terror concerns).

While the Victorian *Charter of Human Rights and Responsibilities Act 2006* (Vic) provides for a right to privacy (s.13), it does give rise to a direct cause of action for invasions of privacy and it is limited to acts of public authorities.

The LIV supports the Australian Law Reform Commission's (ALRC) recommendations in its inquiry on privacy to create a statutory cause of action.[3] The LIV has, however, identified some concerns with the ALRC recommendations and other issues which it highlighted in its submission to the VLRC. A copy of our submission to the VLRC is attached.

[1] See LIV Submission to Victorian Law Reform Commission, 'Inquiry into Surveillance in Public Places' (6 July 2009) at http://www.liv.asn.au/getattachment/5fbfbd52-73fd-46fe-b983-83b88a75d472/Inquiry-into-Surveillance-in-Public-Areas.aspx. See also LIV submission to Australian Law Reform Commission, 'Issues Paper 31 Review of Privacy' (21 February 2007) at http://www.liv.asn.au/getattachment/5858903d-9cb7-4445-91b0-db5cfc0be71f/Issue-Paper-31--Review-of-Privacy.aspx.

[2] For example see *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281

[3] Recommendations 74–1 to 74-7 of the ALRC Report 108 *For Your Information: Australian Privacy Law and Practice* (released 30 May 2008) (ALRC Report) http://www.alrc.gov.au/inquiries/title/alrc108/index.html.

QoN 2 (p27) – 'Best practice' for privacy protections in data retention schemes in other jurisdictions

In light of time constraints, we have not been able to undertake extensive research or form a view on 'best practice' for privacy protections in data retention schemes in other jurisdictions. Set out below is a brief description of how two jurisdictions – the European Union and Canada – have addressed the matter.

European Union

In 2006, the European Union (EU) *Data Retention Directive* (*Directive*) was enacted to facilitate EU cooperation in criminal investigations and provide for the transfer of electronic data between party states.[4] Internet Service Providers and other electronic communications services and networks are expected to store email and phone 'traffic data,' including the identity of the sender and recipient and time of contact, for between six months and two years.[5] State police forces have access to this information subject to requirements of their respective state laws.[6]

Although the *Directive* does not expressly protect human rights, the two following conventions are relevant when analysing whether an individual's right to privacy is appropriately protected when the *Directive* is employed to store and process information:

- *European Convention on Human Rights* (*ECHR*),[7] particularly the right to privacy in Article 8, and
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the *Convention*).[8]

As summarised by Bignami, case law from the European Court of Human Rights and the European Court of Justice renders the storage and processing of personal data pursuant to the *Directive* an interference with the right to privacy unless the three following conditions are satisfied:[9]

1. The storage and processing of data is performed by a public authority or for a public purpose, authorised by law and accessible to the public. Accompanying provisions must preclude arbitrary government interference and require individuals to be notified of a possible interference.
2. The purpose of the storage and processing must be legitimate, that is, related to one of the following purposes in Article 8 of the *ECHR*:
    a. In the interest of national security, public safety or economic well-being of the country,
    b. To prevent disorder or crime,
    c. To protect health or morals, or
    d. To protect the rights and freedoms of others.
3. The Interference must be 'proportional' which considers the least rights-burdensome means of achieving the public purpose and compares the importance of the rights with the public purpose.

[4] See further Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' 8 *Chicago Journal of International Law* (2007-2008) 233 at 238.
[5] *Council Directive 2006/24/EC*, 2006 OJ (l 105) 54, art 3, 6.
[6] Ibid, arts 1, 4 and 8.
[7] *Convention for the Protection of Human Rights and Fundamental Freedoms,* CETS No. 5, Rome (4 November 1950) at http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG (accessed 16 December 2010).
[8] *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* ETS No 108, Strasbourg (28 January 1981).
[9] Francesca Bignami, above n.4, 242-243.

Under point 2, 'legitimate purpose' is restricted in application to investigate and prosecute past crime, rather than prevent future crime. This is because the Working Party tasked with drafting the *Directive* criticised the nearly unfettered access police would have to electronic communication.[10]

Proportionality under point 3 is complex because there are numerous proportionality test formulations and the burden of justification resides with government and varies according to the importance of the right and public purpose in question.[11]

Bignami highlights two features that have helped to reinforce the protection of rights, such as the right to privacy, under the *Directive*:

- The issue of data retention was subject to extensive and high quality public debate prior to the drafting of the *Directive*,[12] and
- In 2007, an independent supervisory body, a European Union Agency for Fundamental Rights, was established to investigate instances of rights abuses in member states.[13]

The flow of electronic communication data out of EU Member states is prohibited unless a non-Member state has adequate privacy safeguards – such as similar data retention legislation – in place.

Canada

Canada's data retention system is principally contained in the *Personal Information Protection and Electronic Documents* Act 2000 (*PIPEDA*). Principle 5 of *PIPEDA* provides for data retention for a limited period of time. Sections of this data retention principle were influenced by the *OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data*. The Canadian data retention principle provides that:[14]

> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

The principle is similar to the *Directive* as it focuses on data retention rather than use, applies a test of necessity to that retention and is connected to the purpose for which the data was collected.[15]

PIPEDA has been criticised however for the following deficiencies:[16]

- High level of generality.
- Ineffective oversight mechanisms.
- Ineffective enforcement mechanisms.
- Limited applicability. For example, it does not apply to not-for-profit organisations in the private sector.
- Peculiar relationship with provincial legislation. *PIPEDA* does not apply if the federal cabinet deems applicable provincial privacy legislation to be "substantially similar".
- Non-mandatory development of guidelines by organisations which include minimum and maximum retention periods. [17]

Restrictions on data retention have applied to federal public entities in Canada since 2000 and, more recently, to the private sector.[18]

---

[10] Francesca Bignami, above 4, 245; see *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive*, 2002/58/EC (COM(2005) 438 final of 21.09.2005) (21 October 2005) 8 at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_en.pdf (accessed 14 December 2010)
[11] Francesca Bignami, above n 4, 246.
[12] Ibid, 253.
[13] See Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, 2007 OJ (L 53) 1 at http://www.fra.europa.eu/fraWebsite/attachments/reg_168-2007_en.pdf (accessed 14 December 2010)
[14] *Personal Information Protection and Electronic Documents* Act 2000, s 4(5) (*PIPEDA*).
[15] Jeremy Warner, 'The Rights to Oblivion: Data Retention from Canada to Europe in Three Backward Steps' [2005] 2 *University of Ottawa Law and Technology Journal* 75, 97
[16] Ibid, 92.
[17] *Personal Information Protection and Electronic Documents Act* 2000 (Can).

QoN 3 (p.32) Scope for proper and genuine consent to use of personal data in an online context

A number of factors affect an individual's ability to provide proper and genuine consent to the use of personal data in an online context. Given the time constraints, we have focused our answer on: terms and conditions; "disproportionate" consent; and the use of cookies by advertisers to create online profiles of consumers.

Terms and conditions

We agree with the concerns raised by the Committee that terms and conditions for websites and accessing online goods and services are often complicated and can be an impediment to genuine consent. The trend for legal documents to be written in plain English, especially common transactional documents such as terms and conditions, is increasing. However, long and complex terms and conditions persist in the online world.

The length and complexity of terms and conditions is concerning and raises questions about the genuineness of an online user's consent. It would be reasonable to question the ability of a person to give genuine consent to a document which is long and covers matters as complicated as cross-jurisdictional copyright, privacy and licensing arrangements. This question is even stronger when applied to changes to some terms and conditions. Online companies will generally notify users that the terms and conditions have been changed. However, some online companies do not highlight the changes made (e.g. through the use of tracked changes or similar). Instead, they direct the user to the complete terms and conditions, requiring them to read them in their entirety every time a clause in the terms and conditions is amended.

Terms and conditions are not the appropriate place to deal with matters of privacy. Dealing with privacy in terms and conditions suggests that privacy is another commodity that can be traded between equal parties. This is not the case. Collecting personal information imposes obligations on the organisation collecting the information. Information regarding privacy should explain how those obligations are being satisfied. It might be more appropriate to require organisations to address privacy issues in a separate document which addresses how the organisation is complying with each of the National Privacy Principles (and, if passed, the Australian Privacy Principles).

Disproportionate consent

"Disproportionate consent" refers to the situation where the extent to which individuals must "consent" to their privacy being waived or given up is disproportionate to the service being provided. Examples include: the provision of credit card details for "free" trials; provision of date of birth and address information to access a purely online product with no physical delivery requirements; and agreeing to cookies accessing an individual's computer, where those cookies do not improve the service received by the individual.[19]

Disproportionate consent calls into question the genuineness of the consent. We consider that organisations should be restricted to seeking private information and consent to its use only to the extent that it is reasonable and proportionate to the service being accessed.

Building profiles

The Committee referred to the practice of some organisations using cookies to build online profiles of individuals. Our ability to comment on this practice is restricted by our limited understanding of

[18] Jeremy Warner, above n 15, 78.

[19] It is accepted that some cookies facilitate or improve the service provided to individuals, especially where pages are accessed on a regular basis.

the details of this practice. Whether consent to such practices can ever be genuine depends on matters such as whether the practice is supported by a contractual agreement between the organisation running the website and the organisation building the profile; whether either or both of those organisations conducts business in Australia, such that the National Privacy Principles apply; and whether the purported consent is given by the individual to the organisation running the website or the organisation building the profile.

The Committee's concerns about this practice – and other issues raised by the Committee – could be raised in a reference to the Privacy Commissioner to undertake research into these practices. Section 27A(1)(c) of the Privacy Act 1988 provides that one of the functions of the Privacy Commissioner is to 'undertake research into, and to monitor developments in, data processing and computer technology (including data-matching and data-linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring'. The Privacy Commissioner could be asked to determine the effects of profile building technology on the privacy of individuals and whether the organisations involved are complying with their obligations (if any) under the National Privacy Principles.

QoN 4 (pp32-3) Privacy in the Workplace

Privacy in the workplace is typically treated as a matter to be regulated as part of the employer-employee relationship. As the line between work and private lives blurs, questions are raised about the extent to which an employer can control employees outside of work hours (e.g. by limiting their involvement in online discussion forums for fear that it will adversely affect the reputation of the employer) and the extent to which an employer can take into account when dealing with workplace matters an individual's conduct in their private lives (e.g. should employers be permitted to discipline an employee for publishing personal but inappropriate photos on a social networking site?).

Where the issues involve individuals in their capacity as private citizens, rather than employees, it might be appropriate to enact statutory protections for privacy, rather than continuing to resolve the matter through employer-employee agreements. Questions of an individual's reasonable expectation of privacy and the extent to which people's roles as citizens can be subordinated to their roles as employees are questions of public importance which deserve further consideration.

The Committee may wish to refer to the Victorian Law Reform Commission's report on Workplace Privacy[20] – and the LIV's submission to the VLRC on that issue[21] – in its consideration of this matter.

[20] Victorian Law Reform Commission, Workplace Privacy: Final Report tabled in Parliament on 5 October 2005 http://www.lawreform.vic.gov.au/wps/wcm/connect/justlib/law+reform/home/completed+projects/workplace+privacy/lawreform+-+workplace+privacy+-+final+report

[21] LIV Submission to Victorian Law Reform Commission, 'Response to Victorian Law Reform Commission *Workplace Privacy Options Paper*' (2 February 2005) https://www.liv.asn.au/members/sections/submissions/20050203_8/2.2.05_word.pdf