SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **41**

SUBMITTER

Internet Society of Australia (ISOC-AU)

Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

C/- Maddocks, Level 7, 140 William Street
Melbourne, Victoria 3000
Accounts: P.O. Box 351, Glenorie NSW Australia 2157

To: Senate Finance and Public Administration Committee

Parliament House, Canberra

By email: fpa.sen@aph.gov.au

6 October 2010

EXPOSURE DRAFT OF AUSTRALIAN PRIVACY AMENDMENT LEGISLATION

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to comment on the Exposure Draft of the Australian Privacy Amendment Legislation.

ISOC-AU is a non-profit society founded in 1996, which promotes the Internet development in Australia for the whole community. ISOC-AU is a chapter of the worldwide Internet Society and is a peak body organisation, representing the interests of Internet users in Australia.

ISOC-AU's fundamental belief is that the Internet is for everyone. We provide broad-based representation of the Australian Internet community both nationally and internationally from a user perspective and a sound technical base. We have a longstanding and ongoing commitment to the effective representation of these interests in self-regulatory processes in the telecommunications, domain name and Internet-related services industries.
We also consistently promote the availability of access to the Internet for all Australians.

This Draft Privacy Amendment legislation includes the proposed new Australian Privacy Principles. While all of the Privacy Principles are important for adequate privacy protection in Australia, this submission addresses two principles of particular importance to Internet users: Principle 2 on Anonymity and Pseudonymity and Principle 8 on Cross Border Disclosure of Personal Information.

1. Introduction

There can be little dispute that new technologies have significantly increased the possibility of personal information being collected, collated, matched and disseminated in ways that significantly impact on the protection of personal information. Over 15 years ago, the Privacy Commissioner's Office published a series in information papers that looked both at the impact of new technologies on privacy, and community attitudes towards the risks of new technologies on an individual's privacy.

As the Privacy Commissioner's Office found:

> New communications networks and services have created a number of risks to personal information privacy that have either previously not existed, or have not existed on the scale which is now emerging. Risks to personal privacy include the potential re-use of personal information for purposes other than those for which it was given, unauthorised access to personal information in networks, insecure storage of data, poor quality personal information being used as a result of communications activities that occur without the knowledge of the individuals concerned and without mechanisms for it to be corrected, and issues relating to intrusive communications products and services.[1]

Public attitudes to new technologies, particularly computers, reflect the growing awareness of the risks to privacy that new technologies pose. In surveying those community attitudes, the Privacy Commissioner's Office found that some of the highest risks people felt to their privacy include the following:

- Computers are seen as a major threat to privacy. When asked about computers, more than 70 per cent feel that they are reducing the level of privacy in Australia.
- Nearly 80 per cent think computers have made it easier for confidential personal details to fall into the wrong hands.
- Only a small minority believe there are adequate safeguards for personal information kept on computer, and only one in five are confident they understand how new technologies could affect their personal privacy.[2]

Indeed, the Privacy Commissioner's recent handling of privacy issues involving both Facebook and Google suggest that privacy is more, not less of an issue since those Information Papers were published.

2. Anonymity and Pseudonymity

The existing National Privacy Principles provide a principle of anonymity as follows:

> Anonymity: Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

The proposed new Privacy Principle adds the concept on pseudonymity as follows:

> Privacy Principle 2:
> (1) Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity
> (2) Subsection (1) does not apply if ….
> (b) it is impracticable for an entity to deal with individuals who have not identified themselves.

The addition of pseudonymity is a significant improvement on the existing Anonymity Principle. Increasingly, for online information and transactions, to obtain the information or complete the transaction, one must fill in required information fields. Allowing pseudonymity allows the information to be provided or the transaction to be completed without unnecessary personal information being provided.

---

[1] Office of the Privacy Commissioner, Privacy Implications of New Communications Networks and Services: Information Paper No. 1, August 1994, p. 4

[2] Office of the Privacy Commissioner, Community Attitudes to Privacy: Information Paper No. 3, August 1995, p. i.

The test of 'practicability' or, in the proposed new principle, the test of 'impracticability' undermines the principle. It may be impracticable for an entity to change the information fields it requires, or otherwise collects. But if the information is not reasonably necessary to the information to be provided, or the transaction to be completed, the information should not have been required in the first place.

The Companion Guide to the draft principles stresses the importance of 'first considering whether it is necessary to collect personal information at all'. Indeed, the Guide says that in some circumstances, 'particularly on the Internet' it is not necessary for a person to identify themselves.[3] However, the Guide does not explain what the test of impracticable might mean in light of that overarching principle, instead suggesting that the Privacy Commissioner will be 'encouraged' to define what impracticable might mean.

If the basic principle is to only collect personal information that is reasonably necessary for one of the entity's functions or activities, then anonymity or pseudonymity should be permitted unless the collection is authorised or required by law, a court or tribunal or is reasonably necessary for one of the entities functions or activities.

Recommendation:
Subsection (2)(b) be changed so that this exception to the principle on anonymity and pseudonymity is only allowed if the collection of correct personal information is reasonably necessary for one of the entity's functions or activities.

3. Cross Border Disclosure

The proposed Privacy Principle 9 requires that, before an entity discloses personal information outside of Australia (where the overseas disclosure is not to the entity itself), the entity must take such steps that are reasonable in the circumstances to ensure that the overseas entity does not breach the Australian Privacy Principles. One of the important exceptions to the principle is when the overseas recipient of the information is subject to a law or binding scheme that protects personal information in away that is substantially similar to protection afforded in Australia, and the affected individual has a way to enforce the overseas privacy protection.

Our concern is that individuals and small businesses are unlikely to have the resources to ascertain whether overseas entities are subject to privacy laws or enforceable schemes that provide 'substantially similar' privacy protection to that provided by Australia. There is also no guidance as to that constitutes 'reasonable steps' that an entity must take to ascertain what privacy protection will in place if that individual or entity transfers personal information overseas.

Recommendation:
The Privacy Commissioner be required to issue guidelines on two issues:

- **What constitutes 'reasonable steps' that an entity must take before transferring personal information outside of Australia; and**
- **What are the overseas jurisdictions where privacy protection under law or a binding scheme is 'substantially similar' to the privacy protection in force in Australia.**

[3] Australian Government, Companion Guide: Australian Privacy Principles, June 2010, p. 9

We will be happy to provide further comments on issues raised by this Consultation Paper

Tony Hill
President
Internet Society of Australia
President@isoc-au.org.au

Holly Raiche
Executive Director
Internet Society of Australia
ed@isoc-au.org.au