Law Institute Victoria

Committee Secretary
Senate Standing Committee on Environment, Communications and the Arts
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

By email to eca.sen@aph.gov.au

Dear Committee Secretary

**The adequacy of protections for the privacy of Australians online**

The Law Institute of Victoria (LIV) notes recent media reports that the Attorney-General's Department has been in discussions with industry on implementing a data retention regime in Australia (the data retention proposal).[1] Such a regime might require internet service providers (ISPs) to log and retain customers' browsing history and email use. This information would then be available to law enforcement agencies to access, when needed. We understand that a data retention regime has been established by the European Union.[2]

The LIV has serious concerns about the data retention proposal, which would have significant consequences for the privacy of individuals. The LIV is also concerned about the way in which this proposal is being developed and, in particular, the lack of public consultation.

**Privacy implications under the National Privacy Principles**

Requiring an ISP to log and retain a customer's browsing history and email use would oblige ISPs to collect and store significant amounts of personal information. The data retention proposal, as reported, would require the collection of *all* internet and email histories for *all* internet users.[3] The LIV considers that the data retention proposal is inconsistent with and represents a significant departure from the National Privacy Principles (NPPs).

The data retention proposal is inconsistent with NPP 1, as it would involve the collection of personal information that is not necessary for a function or activity of the ISP. The information would not be collected for the function of providing an internet service. Rather, the purpose would be collecting information in the event that it *might* prove useful for law enforcement agencies. The LIV submits that the collection of information under the data retention proposal is unnecessary both for the functions of the ISP and for the functions of the ultimate user, law enforcement agencies. Law enforcement agencies can currently obtain internet and email histories of persons suspected of committing crimes by obtaining warrants.

---

[1] ZDNet, "Govt wants ISPs to record browsing history" 11 June 2010 at http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[3] We note that a spokesperson for the Attorney-General has denied that the data retention regime would include collecting individual web browsing history, see *The Age*, "No Minister: 90% of web snoop document censored to stop 'premature unnecessary debate" 23 July 2010 at http://www.theage.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html.

The Law Institute of Victoria is a member of
Law Council of Australia

Law Institute of Victoria Ltd
ABN 32 075 475 731
Ph (03) 9607 9311 Fax (03) 9602 5270
Email lawinst@liv.asn.au
470 Bourke Street Melbourne 3000 Australia
DX 350 Melbourne GPO Box 263C Melbourne 3001
Website www.liv.asn.au

Furthermore, we submit that the collection of *all* internet browsing and email usage of *all* customers, including those not suspected of breaching any laws, is an unreasonably intrusive way of collecting information for the purposes of enforcing laws. The LIV considers this to be unreasonable because it would require the collection of personal information of persons who have not, and are not suspected to have, committed crimes.

Under the data retention proposal, ISPs would be required to collect enormous amounts of information. Such information would presumably be stored in databases. The sheer scale of such databases and the period for which they would need to be stored would render it extremely difficult for ISPs to comply with NPP 4; that is, taking reasonable steps to protect the personal use from misuse, loss and from unauthorised access, modification or disclosure and against other misuse of the personal information.

The data retention proposal also contradicts NPP 4.2. NPP 4.2 requires an organisation to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2. Given that the information is being collected in the event that it *might* be useful to law enforcement agencies at some unspecified time in the future, ISPs would be required to retain the information indefinitely or for the period specified as the data retention period.

The data retention proposal may also be inconsistent with NPP 8, which states that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation. The collection and retention of an individual's entire browsing and email history would render it almost impossible for the individual to remain anonymous.

It is possible that parts of an individual's browsing and email history will contain sensitive information, as defined in s 6 of the *Privacy Act 1988* (Cth). If so, collecting and retaining that information will constitute a potential breach of NPP 10.

**Australian Law Reform Commission recommendations**

The data retention proposal is also inconsistent with the recommendations made by the Australian Law Reform Commission (ALRC) in its recent report *For Your Information: Australian Privacy Law and Practice* (2008) (the ALRC report).

The data retention proposal is inconsistent with the ALRC's recommendation that data be collected only where "necessary". The LIV considers that it is not "necessary" for the enforcement of laws that all internet and email usage be logged and retained. It might be helpful for law enforcement agencies to access such information; however, it is not necessary. As identified above, the internet and email usage of a person suspected of committing crimes can be obtained under current legislation, particularly through the issuing of warrants.

The large-scale collection of personal information by governments because it *may* be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet. By way of illustration, the LIV suggests that neither government nor community would tolerate proposals to place telephone intercepts on all phone lines in Australia and record all conversations, or to open all mail, in case such information may be of use to law enforcement agencies. Such proposals would be unacceptable in a democratic society. There is no demonstrable reason why internet communications should be treated differently to other communications.

In any event, the LIV considers that the data retention proposal would in reality be unworkable for law enforcement agencies. The amount of information collected and retained by ISPs would overwhelm law enforcement agencies. It is highly unlikely that law enforcement agencies would have the resources to search through information in order to detect crimes at first instance. It is more likely that information would be sought in the context of an ongoing investigation, where the identity of suspects are already known or suspected. In such instances, the current procedures for the issuing of warrants are satisfactory. Such procedures provide law enforcement agencies with the information they require, while maintaining the personal privacy of those not involved in crimes and ensuring that any infringement on personal privacy is done only with the oversight of a judge or tribunal member.

**Process concerns**

The LIV is also concerned that such a proposal with significant implications for personal privacy might be developed before the government has fully responded to the ALRC report. The ALRC Report was published in 2008 and the government delivered its "first stage" response in October 2009. The first tranche of recommendations have only recently been referred to the Senate Finance and Public Administration Committee for consideration.[4] Formal adoption and action on the ALRC report appears to be some years away.

The data retention proposal is one of many examples of a government keenly adopting proposals that interfere with personal privacy, while delaying and deferring important reforms that would better protect personal privacy. This is unfortunate, as the personal privacy of citizens is a fundamental human right and should be paramount in a democracy. It should certainly take higher priority than the convenience of government agencies.

The LIV is also concerned about reports that the government is engaging in discussions with industry in respect of the data retention proposal, rather than discussing the proposal with the community. It is also concerning that the government is reported to be claiming exemptions under the *Freedom of Information Act 1982* (Cth) in respect of documents relating to these discussions, on the basis that releasing these documents "may lead to premature unnecessary debate and could potentially prejudice and impede government decision making".[5] The LIV considers that such debate is necessary and calls for adequate citizen engagement during the development stage of any proposals affecting privacy, not after a proposal is a fait acompli.

Yours faithfully,

**Steven Stevens**
President
Law Institue of Victoria

CC: Commonwealth Attorney-General

---

[4] Senate Finance and Public Administration Committee Inquiry into the Exposure Drafts of Australian Privacy Amendment Legislation, at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm

[5] See *The Age*, "No Minister: 90% of web snoop document censored to stop 'premature unnecessary debate" above n3.