23 August 2012

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

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

Dear Committee Secretary

***Inquiry into the* Privacy Amendment (Enhancing Privacy Protection) Bill 2012 *(Cth)* – questions on notice**

Thank you for the opportunity for Katie Miller to appear before the Committee on behalf of the Law Institute of Victoria (LIV) to answer questions on our submission to the Committee's inquiry into the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) (the Bill) (submission number 8).

We provide the following responses to the written questions on notice from the Committee, sent to us by email on 16 August.

Question 1: Several APPs contain different tests or standards for government agencies and other organisations in relation to the collection, use and storage of personal information. Are these differing standards justified? If not, what amendments to the bill are required to remedy this?

A major reform in the Bill is the consolidation of the current Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) into one set of privacy principles, the 'Australian Privacy Principles' (APPs) based on recommendation 18–2 of the Australian Law Reform Commission report, *For Your Information: Australian Privacy Law and Practice* (the ALRC report).

The ALRC report (at [18.87]) lists a number of benefits that are likely to flow from this reform, including that it would:

- foster national and international consistency in privacy regulation; and
- clarify and simplify the obligations of agencies and organisations with respect to information privacy, in particular where an organisation is acting as a contracted service provider or is involved in a public-private partnership, it would reduce significantly the problems associated with the organisation having to comply with both the IPPs and NPPs.

The ALRC report found, however, that the new consolidated principles should not apply rigidly to both agencies and organisations, and that some principles in the UPPs should apply only to organisations (at [18.88]). The ALRC report discusses particular areas where different standards might be justified for agencies and organisations: direct marketing and government related identifiers.

We consider that different standards are justified for agencies and organisations only in a small number of limited areas, where there are reasons for a different approach because of the nature of government activities and the need to regulate certain uses of personal information more stringently than others.

In relation to direct marketing, the ALRC report discusses the need for government agencies to be able to directly market government services to the public (at [26.34] - [26.48]). However, the ALRC also acknowledges that where an agency is in fact a commercial operation, in competition with the private sector, they should be required to comply with the same standards for direct marketing.

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

Further, the ALRC report highlights (at [30.19] – [30-23]) that a special approach is required in relation to government related identifiers, to accommodate the situation where an agency creates the identifier and then shares this with an organisation for a specific purpose – so that it is the organisation (rather than the agency) that must comply with proposed APP 9 (the agency already being bound by strict confidentiality provisions in the legislation creating the identifier).

The Bill, however, maintains different tests or standards between organisations and agencies in other areas beyond direct marketing and identifiers (for example, in APP3.3(a)) and therefore largely reflects the current differences in standards between the NPPs and IPPs. These different standards undermine the uniformity of the APPs and reduce the benefit of consolidating the principles. In addition, we are concerned that the different standards make it very difficult for individuals to understand their privacy rights.

The current approach to privacy protection in the *Privacy Act* 1988 (Cth) focusses on regulating the entities collecting personal information. The APPs therefore approach privacy from the perspective of the entity, regulating what they can and cannot do, and not from the perspective of the individual.

While some agencies are specifically empowered by legislation to collect and use personal information, it does not follow that they will necessarily obtain more or less personal information than other agencies or organisations. For example, some private organisations now collect significant volumes of personal information through individual use of the internet, where notions of consent and 'informed consent' are less stringent than in the past. It would therefore seem difficult to justify a different privacy standard based only on whether the entity is an agency or organisation.

We submit that individuals should generally be able to expect the same level of protection for personal information, and in particular sensitive information, regardless of the type of entity collecting the information. Rather than focussing on permissible use of information by organisations as compared to permissible use by agencies, the APPs should start from the perspective of the individual. Under an individual approach to privacy, any distinctions in levels of privacy protections should be based on the nature of the information (and perhaps also the nature and extent of consent given by the individual), rather than on the entity collecting the information. Under this approach, sensitive information should have more protection (as it does now) and individuals should be able to consent to lower standards of protection (for example,. they may exchange convenience or processing times for a lower standard of privacy).

The LIV submits that the Bill should be amended to establish one standard test, so that each APP refers only to the obligations of an entity (with the exception of APP 7 and 9 which deal with direct marketing and government related identifies). We agree with the submission of the Office of the Australian Information Commissioner (OAIC) that a requirement that the collection be 'necessary' is sufficient for both agencies and organisations (submission 47, at [42]).

The APPs should then be redrafted to include levels of protection depending on the nature of the information and consent given. For example, levels of protection for: sensitive information, non-sensitive personal information obtained by consent, non-sensitive personal information obtained by coercive means (ie authorised by legislation – this would apply to law enforcement agencies, for example) and then all other information. Each APP could identify at the outset which subset of information it applies to. This might also make it easier to apply the APPs.

Question 2: The OAIC argued in its submission that exemptions for government agencies should be set out in those agencies' enabling legislation, rather than in the APPs themselves. What is your view on this suggestion?

The LIV agrees with the OAIC's emphasis on the importance of having a single set of high level principles for the public and private sectors which promote national consistency and minimise complexity.

Our preference would be for the any exemptions for government agencies to be set out in a schedule to the *Privacy Act*, rather than in enabling legislation, to maintain uniformity in the APP but also to

make it easier to identify those agencies with specific exemptions. An example of this approach can be found in Schedules 1 and 2 to the *Administrative Decision (Judicial review) Act (*Cth) 1977, which set out classes of decisions that are not decisions to which the Act/ part of the Act applies.

Question 3: Your submission argues that the definition of 'consent' in the Privacy Act requires further development and clarification. Do you have any specific proposed amendments that would satisfy your concerns regarding this definition?

The *Privacy Act* currently defines consent to mean express and implied consent (in s6). Consent is required under the APP, for example, under APP 3 in relation to the collection of solicited sensitive information.

In our submission, we argue that consent to provide information should not be obtained in a coercive or unreasonable way and that provision of goods and services should not be made conditional on consenting to the provision of information which is unrelated to the provision of the good/service.

Consent should not be assumed but has to be proven by express or implied acts or words. Informing a person that a particular act will be taken as consent is not the same thing as establishing that the person actually consented, especially where it is not clear whether the person was aware of, understood or accepted the organisation's statement that a particular act would be taken as consent. One example, described by Katie Miller in her evidence to the Committee, is where a pub or club informs a patron that, by entering the premises, s/he consents to their ID being scanned and retained on file for 28 days. That is, consent cannot be deemed unilaterally by the entity.

Accordingly, we submit that the *Privacy Act* should be amended to clarify that:

- consent should be limited to collection of information necessary for the transaction between the individual and entity.;
- an individual should never be required to consent to an effective abdication of their rights under the APPs; and
- consent must be informed consent.

Additional comments on social media

The LIV also wishes to provide further comments to the Committee in relation to the rapid growth of social media and Senator Humphries' questions during the public hearing regarding concerns raised by social media companies about potential breaches of direct marketing provisions in the Bill by individuals using social media.

The Bill is an important first step in implementing the recommendations of ALRC report. However, regulation of social media, and consideration of its interaction with privacy laws, is a significant gap in the Bill because the ALRC report was published in 2008, prior to the burgeoning of social media and the consequential challenges to traditional legal approaches to protecting privacy.

Privacy laws in Australia, including the Bill, do not create a statutory right to privacy, but rather, regulate the collection, use and disclosure of personal information. Privacy laws generally focus on two major collectors of information, with the aim of preventing the misuse of data: government and private sector businesses. The rise of social media challenges traditional conceptions about who is collecting personal information and for what purposes, and raises the question of who should bear responsibility for protecting privacy of personal information.

The LIV agrees that further consideration needs to be given to how privacy laws should regulate social media.

Social media companies play different roles with respect to the activities of individual users. Sometimes, they will be 'neutral' and merely provide a platform for publication and collection of information. At other times, they will have a more active role in moderating publication of information and often, they will also collect and use information themselves. In all roles, the policies and practices of the social media company will impact on how individuals are able to interact in the online platform, including by influencing how personal information might be collected by individuals and how consent is sought.

We do not support any proposal to simply provide an exemption for social media companies for liability for the activities of individual users of social media, as clearly, social media companies are able to influence how individuals use their service. We appreciate, however, that alternate approaches to compliance and liability for protecting the privacy of personal information might be necessary. Approaches to consider could be to require social media companies to establish internal dispute processes to receive complaints from individual users about breaches by other users. Where a complaint meets a particular threshold, the social media company could be required to refer the matter to the Privacy Commissioner.

We acknowledge that further complexity arises where individuals and/or social media companies are operating outside of Australia, and the global nature of the internet warrants further consideration in this context.

Ultimately, the government will need to make a policy decision about whether individuals are intended to be covered by the *Privacy Act*, when participating in social media for private purposes only.

Please contact , Lawyer for the Administrative Law and Human Rights Section, on in relation to this submission.

Yours sincerely,

Michael Holcroft
President
Law Institute of Victoria