THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: HumanRights:JDvk795025

21 November 2013

Ms Sabina Wynn
The Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001

By email: privacy@alrc.gov.au

Dear Ms Wynn,

ALRC Inquiry into Serious Invasions of Privacy in the Digital Era

I am writing to you on behalf of the Human Rights Committee of the Law Society of NSW ("Committee"), which has the responsibility to consider and monitor Australia's obligations under international law in respect of human rights; to consider reform proposals and draft legislation with respect to issues of human rights; and to advise the Law Society on any proposed changes.

The Committee thanks Ms Tina O'Brien for indicating that submissions will be accepted after the due date.

The Committee refers to the Issues Paper, *Serious Invasions of Privacy in the Digital Era* ("Issues Paper") prepared by the Australian Law Reform Commission ("ALRC").

The Committee provided a submission in response to the Department of Prime Minister and Cabinet 2011 Issues Paper, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*. In this submission the Committee set out its general views in relation to a statutory cause of action for serious invasion of privacy, including noting an individual's right to privacy under Article 17 of the *International Covenant on Civil and Political Rights*. The Committee noted in that submission that introduction of such a cause of action may conflict with the ICCPR right of freedom of expression (Article 19). The cause of action would therefore need to be tailored to balance that right with the new cause of action, to the extent they conflict. As the submission has relevance to the issues under inquiry here (particularly to questions 7, 9 and 16), it is attached for your information.

In addition, the Committee notes that at question 2 of the Issues Paper, the ALRC requests responses on the specific types of activities a statutory cause of action for serious invasion of privacy should prevent or redress, where the current law may be inadequate (question 2 of the Issues Paper). The Committee provides its comments, in relation to information collection and use by private entities, as well as by governments.

1. Information collected and used by private entities

In the Issues Paper at p 14, it is noted that organisations have a "rapidly expanded technological capacity" to:

> track the physical location and activities of individuals, to collect and use information from social media, to aggregate data from many sources, and to intercept and interpret the details of communications.

In response to this question, the Committee notes its privacy concerns in relation to large scale data mining. Through the use of online and social media products, individuals are having to exchange personal information for the benefit obtained from the products. Australian citizens are almost certainly providing information to organisations that operate in different jurisdictions. The Committee submits that the ALRC's inquiry should consider the question of how Australian law operates to protect individuals' personal information that may be bought, sold and used, including in foreign jurisdictions (noting that domestic protections of privacy could be weaker in those jurisdictions).

In particular, the Committee notes that the resulting pool of data allows organisations to undertake big data analytics to categorise and organise information which can be used to, for example, identify trends, forecast behaviour and market products in a more targeted way. While the Committee acknowledges that this may be a question that is outside the scope of a legislative exercise, the Committee is concerned that the practice of big data analytics presents a threat to an individual's right to privacy in subtle ways. Professor Joseph W. Jerome argues that:

> In the end, the worry may not be so much about having information gathered about us, but rather being sorted into the wrong or disfavored bucket. Take the example of an Atlanta man who returned from his honeymoon to find his credit limit slashed from $10,800 to $3,800 simply because he had used his credit card at places where other people were likely to have a poor repayment history.
>
> Once everyone is categorized into granular socioeconomic buckets, we are on our way to a transparent society. Social rules of civility are replaced by information efficiencies. While this dynamic may produce a number of very significant societal and communal benefits, these benefits will not fall evenly on all people. As Helen Nissenbaum has explained, "the needs of wealthy government actors and business enterprises are far more salient drivers of their information offerings, resulting in a playing field that is far from even." Big data could effectuate a democratization of information but, generally, information is a more potent tool in the hands of the powerful.
>
> Thus, categorization and classification threaten to place a privacy squeeze on the middle class as well as the poor. Increasingly large swaths of people have little recourse or ability to manage how their data is used. Encouraging people to contemplate how their information can be used—and how best to protect their privacy—is a positive step, but a public education campaign, while laudable, may be unrealistic. Social networks, cellular phones, and credit cards—the lifeblood of the big data economy—are necessities of modern life, and assuming it was either realistic or beneficial to get average people to unplug, an overworked, economically insecure middle class does not have the time or energy to prioritize what is left of their privacy. [footnotes in the original deleted][1]

---

[1] Joseph W. Jerome. "Buying and selling privacy: big data's different burdens and benefits" (3 September 2013) 66 *Stanford Law Review Online* 47 available online: http://www.stanfordlawreview.org/online/privacy-and-big-data/buying-and-selling-privacy (accessed 1 November 2013).

To this end, the Committee notes that UN Human Rights Committee's General Comment No. 16 on Article 17 of the ICCPR General Comment No. 16 provides at [10] that:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

2. Information collected and used by foreign governments

In addition to its concerns about data mining and big data analytics carried out by private organisations, the Committee notes its serious concerns in relation to the recent reports that the large scale unauthorised international surveillance and data mining program carried out by the US National Security Agency[2] included the unauthorised surveillance of Australian citizens.

Article 17 of the ICCPR places a positive duty on State parties to guarantee the secrecy of correspondence through legislative and administrative mechanisms. The Committee notes that UN Human Rights Committee's General Comment No. 16 on Article 17 of the ICCPR[3] states at [8] that:

> Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.

This raises the question of what avenues of action are available to individuals in the instance of foreign powers using the internet to engage in wholesale surveillance of Australian citizens. The Committee notes also that there are reports that the Attorney-General's Department is aware of the unauthorised surveillance program,[4] and that Australian Defence Signals Directorate cooperated with the unauthorised surveillance of Australian citizens, as well as of nationals of other countries.[5] The

---

[2] See for example, Nick O'Malley and Ben Grubb, "US Government Electronic Surveillance: Australians at Risk" 7 June 2013, *Sydney Morning Herald*, available online: http://www.smh.com.au/it-pro/security-it/australians-at-risk-in-us-electronic-surveillance-program-20130607-2ntwj.html (accessed 1 November 2013).

[3] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, available at: http://www.refworld.org/docid/453883f922.html (accessed 4 November 2013)

[4] "Attorney-General's Department briefs Minister in March on PRISM allegations" 8 October 2013, Transcript of *AM with Tony Eastley* available online: http://www.abc.net.au/am/content/2013/s3864183.htm (accessed 1 November 2013).

[5] See for example David Wroe and Ben Grubb, "Australia collecting data for NSA, leaks show" 16 October 2013,*Sydney Morning Herald* available online: http://www.smh.com.au/it-

Committee submits that one way to address this issue might be to extend the statutory cause of action to include a right to sue the Crown and any foreign power that might be putting Australian citizens under surveillance, whether via the internet or through other means. However, if the ALRC does not favour this option, the Committee would be grateful for the ALRC's consideration and recommendation(s) in relation to this issue.

In this context the Committee notes the principles of the decision of *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 may apply. In that case, an American publisher was held liable for defamation in Australia where an Australian citizen was defamed online. The effect of this decision is that applicants could bring an action for defamation on the internet against any defendant, regardless of the defendant's location.

The Committee thanks you for the opportunity to provide comment. Please contact Vicky Kuek, policy lawyer for the Committee, if you have any questions. She is available on victoria.kuek@lawsociety.com.au or (02) 9926 0354.

Yours sincerely,

John Dobson
President

pro/security-it/australia-collecting-data-for-nsa-leaks-show-20131015-hv24k.html (accessed 1 November 2013).

THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: SW:576588

7 November 2011

The Privacy and FOI Policy Branch
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

BY EMAIL ONLY: privacycauseofaction@pmc.gov.au

Dear Sir/Madam,

Issues Paper – "A Commonwealth statutory cause of action for serious invasion of privacy"

The Human Rights Committee (the "Committee") of the Law Society of NSW has requested that I write to you in relation to the issue of a statutory cause of action for serious invasion of privacy. The Committee has responsibility to consider and monitor Australia's obligations under international law in respect of human rights; to consider reform proposals and draft legislation with respect to issues of human rights; and to advise the Law Society of NSW on any proposed changes. The Committee is a long-established committee of the Society, comprised of experienced and specialist practitioners drawn from the ranks of the Society's members who act for the various stakeholders in all areas of human rights law in this State.

I note that the Law Society of NSW previously submitted on this issue in 2007 with the view that it was unnecessary to provide for a statutory cause of action for serious invasion of privacy. Since that time, the Australian Law Reform Commission (ALRC) and the New South Wales Law Reform Commission (NSWLRC) have both issued reports in relation to privacy (referred to in more detail below). The Committee has had regard to the recommendations set out in those reports and while it acknowledges that this is a complex issue, the view set out in this submission is that a statutory cause of action for the serious invasion of privacy should be introduced.

The Committee's comments are as follows:

1. Australia ratified the International Covenant on Civil and Political Rights ("ICCPR"), the main international human rights treaty, in 1980 and at that time adopted an obligation under international law to implement into our domestic laws, the provisions of that treaty. Article 17 of the ICCPR commits our governments to legislate to prevent a person being "subjected to arbitrary or unlawful interference with his privacy...". Further, Article 2(3) of the ICCPR provides that a person whose ICCPR rights are infringed should be provided with "an effective remedy".

2. Noting that there is no generally applicable cause of action in Australian law for serious invasion of privacy, the Committee is strongly of the view that a

statutory cause of action should be introduced to, inter alia, correct the deficiency in implementing the provisions of the ICCPR in this respect.

3. The Committee refers to the report of the ALRC, Report 108 – "For Your Information: Australian Privacy Law and Practice", 2008 (the "ALRC Report") and generally supports the report's recommendations in respect of the introduction of such a statutory cause of action. The Committee recommends that any proposed legislation should follow those recommendations with certain qualifications, referred to below.

4. The introduction of such a cause of action may conflict with the ICCPR right of freedom of expression (Article 19). The cause of action would therefore need to be tailored to balance that right with the new cause of action, to the extent they conflict.

5. The Committee supports the suggestion of the Victorian Law Reform Commission in its report "Surveillance in Public Places: Final Report 18", 2010 to the effect that there should be a public interest defence to the proposed cause of action which would enable the balancing of the public interest in maintaining a claim in privacy with the interest of the public to be informed about matters of public concern and to allow and protect freedom of expression.

6. The Committee further agrees with the Victorian Law Reform Commission's view in its report that the cause of action should not be restricted to intentional or reckless acts but should, in appropriate cases, extend to grossly negligent acts.

7. The NSWLRC in its "Report 120: Invasion of Privacy", 2009, recommended that damages for such a cause of action should be capped in relation to non-economic loss. The Committee agrees with that recommendation. The cap should be tailored, as far as possible, to avoid different caps being prescribed for the proposed cause of action and actions for defamation, to prevent "cause of action shopping". However, the Committee cautions against a damages cap that is set too low such that the cause of action will not be fully compensatory.

The Committee thanks you for this opportunity to respond to the Issues Paper and for your time in considering this submission.

The Committee would appreciate an opportunity to comment on any draft legislation proposed, with a view to assisting the enhancement of the protection of the fundamental right to privacy in this country.

Yours sincerely,

Stuart Westgarth
President

CC: Law Council of Australia