CYBERSPACE LAW & POLICY COMMUNITY

15 November 2013

Professor Barbara McDonald
Commissioner
Australian Law Reform Commission
c/- tina.obrien@alrc.gov.au

Dear Professor McDonald,

Privacy cause of action – first submission

This is a short initial submission. We will be making more substantial submissions in response to concrete proposals at the Discussion Paper stage.

We agree with the ALRC's proposal for a private right of action.

The current Australian privacy regime is, from the perspective of the individual subject of the information, often rendered ineffective by lack of any real capacity for individuals to enforce it, and by a model of vast and complex exceptions to its principles, scope and jurisdiction which are themselves already limited by reliance on the 'government and business records' thinking of the 1980s era OECD principles.

A private right of action would be a useful complement to the existing regulatory framework, one which has the potential to enable flexible adaptation to emerging developments in the democratisation and distribution of personal data collection and use arising from the profound changes delivered by digitisation, networking and mass access to ever evolving technologies.

The submission of the Australian Privacy Foundation (APF) makes some useful points in this regard. We generally support their assessment of the issues to consider and the avenues to investigate for solutions, without necessarily endorsing all their observations or submissions in detail.

We believe the real difficulty will be around questions of legislative design. The ALRC is right to require that legislation is "sufficiently flexible to adapt to rapidly changing technologies and capabilities without the need for constant amendments, but at the same time be drafted with sufficient precision and definition to promote certainty as to its application and interpretation". The real difficulty is navigating such difficult waters.

We do not know for certain what data will be stored, how it will be stored or how it will be used in the future. Terminology, concepts and rules that may seem neutral as to technologies will inevitably be chosen based on unconscious assumptions about what is possible and what does occur. And an attempt to ignore current practices may render legal rules less relevant, and less likely to result in the kinds of practical changes that privacy may require. In turn, technological design may be influenced by what designers perceive as legal risks associated with particular ways of doing things (with both positive and negative implications).

Ultimately, flexibility and adaptability may be best ensured by both recognising the need for some ongoing legislative amendments and employing non-legislative regulatory strategies in addition to enactment of (more generally worded) legal rules. We hope to comment after the discussion paper is released on the extent to which the ALRC has achieved its stated goal in this regard.

There are, however, some current issues that we can raise at this stage.

One particular area which the new law must grapple with is online content hosted on massive offshore-owned commercial social networking sites. It is important that the new law adequately fills gaps in the coverage of associated new mechanisms for privacy intrusion. Like all technologies, what we now call "social networking" will continue to evolve. The concept of privacy, and in particular which aspects of it are important in what circumstances, will also continue to evolve (in complex non-linear ways).[1] Neither of these need be problematic, provided the law supports people's right to be informed of, and choose for themselves, the level of disclosures they wish to make and the types of uses they wish to accept. The 'death of privacy' idea pushed by some online publishers and marketers to deprecate the need for remedies is therefore unhelpful.

Privacy law need not prevent a person from knowingly disclosing information personal to themselves. But the fact that some people are happy to do this at present does not argue against the need for such basic protections. It also demonstrates the need for wider awareness of the potential adverse consequences associated with such disclosure. Such education is often not in the commercial interests of operators and promoters. The result is information asymmetry, where the benefits of over-exposure of your own or others' personal information are heavily promoted and obvious, while the risks and costs are obscure, 'uncool' and hidden, tends to undermine and delay an assessment proper balancing risks and benefits by users, contributing a potentially high risk environment. Many of the issues that arise are specific to particular current social media technologies and it is likely that the solution does not lie *solely* in the creation of a statutory cause of action.

In closing, we encourage the commission to make efforts to balance the special pleading of certain sectors of industry, particularly those which have in the last few years tended to overstate concerns about the impact of a private right of action, with what we see as a clear need for effective remedies for the broad population now effectively denied them.

Yours sincerely,
Lyria Bennett Moses
David Vaile

[signed Lyria Bennett Moses, David Vaile]

Cyberspace Law and Policy Community
UNSW Faculty of Law

[1] For instance, the oft-heard notion that young people recently and permanently gave up caring about the privacy and security of their information after being seduced by Facebook's notorious promiscuity is undermined by emerging reports of trends in the reverse direction. Facebook faces "a decrease in daily use, specifically among teens" in favour of services like Whatsapp and SnapChat – which embrace "the virtues of privacy", impermanence, and restriction to real-world friends, and shun advertising – because they now don't want "the whole world to know": Parmy Olson, 'Teenagers say goodbye to Facebook and hello to messenger apps,' *The Guardian*, 10 November 2013.