The Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001
Email: privacy@alrc.gov.au

11 November 2013

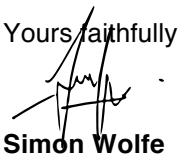
Dear sirs

Re: Submission to the Australian Law Reform Commission's (ALRC) Issues Paper: "Serious invasions of Privacy in the Digital Era"

Please see **annexed** submission to the ALRC, from Blueprint for Free Speech.

For any queries in relation to this submission, or any other matter, please do not hesitate to contact me.

Yours faithfully



Simon Wolfe
Head of Research
E: simon@blueprintforfreespeech.net

Blueprint For Free Speech
PO Box 187, Fitzroy VIC Australia 3065

Submission to the Australian Law Reform Commission's (ALRC) Issues Paper: "Serious invasions of Privacy in the Digital Era (Issues Paper)"

11 November 2013

1 Introduction

We wish to first thank the ALRC for allowing our submission and enabling us to contribute to this important discussion.

Blueprint for Free Speech (**Blueprint**) is an international not-for-profit organisation concentrating on research into "freedoms" law. Our areas of research include public interest disclosure (whistleblowing), defamation, censorship, right to publish, shield laws, media law, internet freedom (net neutrality), intellectual property and freedom of information. We have significant expertise in whistleblowing legislation around the world, with a database of analyses of more than 20 countries' whistleblowing laws, protections and gaps.

We have read and understand the Issues Paper as published in June 2013. Although we understand the Issues Paper to be concerned with twenty-eight separate questions focusing on methods of preventing a serious invasion of privacy, we wish to address what we consider to be four primary matters to be considered by the ALRC in its determinations:

(a) the guiding principles should always be that wherever possible, an individual natural person's privacy should be further protected whereas openness and transparency should be ensured on an institutional, corporate or organisational level;
(b) data sovereignty with respect to the borderless world of cloud computing raises serious and timely issues around individual privacy;
(c) safeguards around 'de-identification' of data are often not enough, and further expert study of the impact of this 'de-identification' process should be conducted;
(d) establishing a cause of action for serious invasions of privacy is a positive step, but it does not necessarily compensate for serious breaches of privacy enabled by other legislation.

2 Individual privacy in conjunction with institutional transparency

When considering the development of any privacy legislation, the concept guiding that process should always be that a natural person's privacy should be protected at all times, and that this should be contrasted from an organisation or institution who should at all times be forced to act transparently and openly.

It follows, therefore, that rights attributed to an individual in respect of privacy should not apply to organisations – they should not be granted the same inalienable right. Additionally, a natural person cannot be expected to have the same level of transparency with their own personal financial information in the same way that a company would have to report its own financial dealings.

The importance of this point is that discussion of the above should not be conflated – that at all times policy makers should be mindful of these two separate, but equally important goals. In fact, if each is properly supported then they will have a symbiotic effect on the other – a strengthening of one will consequently strengthen the other.

3 Importance of data sovereignty

An individual's privacy is ensured by the proper protection of that person's data sovereignty. Data sovereignty is the concept that a person should have control over their personal data – control to distribute, edit, delete or otherwise deal with their data, free from interference from others. The borderless world of cloud computing raises serious and timely issues around individual privacy as it potentially threatens an individual's data sovereignty. Consider, for example, an individual's private medical history. Where once it would have been stored in a filing cabinet in their doctor's office, now they are stored in the cloud. Depending on where, how, and to what level of security it might be held within, this might potentially compromise a person's ability to maintain the sanctity and sovereignty of their personal data, particularly to the standard set by law in their own country. In another context, commercial in confidence information, or perhaps legally privileged material held by a lawyer might easily have its sovereignty threatened where a law firm might outsource all its IT services to cloud servers housed in another country. This is especially so where the business and data relates to matters across borders and a person cannot be sure that the data is secure at its end or storage location. Not only is this an issue for the data sovereignty of particular individuals, it also has the potential to inflict wider micro or macro financial damage to Australia.

The issue of data sovereignty and the need to protect it, and therefore to protect privacy, is an issue that cannot simply be cured by the creation of a cause of action for a serious invasion of privacy. It demonstrates that a more rounded and comprehensive approach is needed. At the very least there should be a consumer support body in Australian responsible for either funding community groups to provide awareness-building of these data sovereignty risks, or else which does it themselves. Without such an organisation, it is very confusing for individuals or small businesses that want to protect the integrity and privacy of their data in the face of data sovereignty risks.

4 Safeguards for 'de-identification'

In the storage of private records, it is often argued that privacy is protected by the removal of key data such as names, and replacing this with an identification number or otherwise masking the identity of the person behind the data. This process is called 'de-identification'. However, safeguards around 'de-identification' of data are often not enough, and further expert study of the impact of this 'de-identification' process should be conducted. Standards about de-identification of individual's information and expert analyst's opinion should be sought on how 'de-identification' might affect the privacy of an individual. Recommended minimum standards of what information must be removed to ensure de-identified data cannot be reassembled should be developed and published for agencies and enterprises alike.

By way of illustration, there is some of the data about a person that would appear not to identify the person (such as post code, gender or date of birth), yet it is possible with high accuracy accuracy to identify the person about whom the data relates despite not having a first or last name. For example, an organisation may remove someone's name from their record, however just having their date of birth, gender and postcode may be enough to identify them anyway. Therefore, it's not true de-identification.

In an era of analytics and big data, there need to be clearly spelt out rules when private data should be de-identified and exactly how it should be de-identified to prevent the reassembly of the identity. If this cannot be done, then people are not often given true privacy, and consequently this may have a chilling effect on freedom of speech.

5 Cause of action for serious invasion of privacy can gloss over how other legislation inhibits privacy

Blueprint welcomes a new cause of action for a serious invasion of privacy. However, this is not the 'silver bullet' for the protection of an individual's privacy. The issue needs a more holistic assessment – how other legislation impacts on a person's privacy, data sovereignty or otherwise. For the purpose of this submission, we do not intend to explore each piece of State and Federal legislation to determine how each might impact on an individual's privacy. However, we wish to illustrate this with an example.

In Schedule 2 of the *Cybercrime Act 2001* (Cth), an individual, even if not under investigation for the commission of a crime, may be required to provide passwords, decrypt or otherwise make readable documents in their possession. This, of itself, is an invasion of privacy (noted also that a cause of action for a serious invasion of privacy would do nothing to limit this). Further, it also creates the potential of forcing someone to incriminate themselves in the commission of another, unrelated offence after the decryption of a document or by divulging a password. The potential impact cannot be known, and a proper assessment of how legislative provisions elsewhere would assist in the proper analysis of serious invasions of privacy.

6 Conclusion

We wish to take the opportunity to once again express how honoured we are to contribute to this process.

Serious invasions of privacy should be avoided, and all tools that enable such invasions to be provided should be strengthened. However, it should be remembered that the creation of a civil cause of action for a serious invasion of privacy is not a silver bullet. A more holistic approach is needed that warns off the creep of legislation potentially damaging an individual's right to privacy.

Blueprint for Free Speech
11 November 2013