98._org_ UNSW Cyberspace Law and Policy Community

Name of organisation: UNSW Cyberspace Law and Policy Community

Proposal 4.1:

The Cyberspace Law and Policy Community supports the ALRC's proposal for a new statutory cause of action for serious invasion of privacy. It is a critical step in protecting an important social value that is otherwise insufficiently protected through existing law.

Proposal 4–2 :

N/A

Proposal 5–1 :

N/A

Proposal 5–2 :

The importance of individual privacy in our society and the significant harm which can be caused when it is compromised requires careful balancing and protection. As the reach, scope and applications to which personal information can be utilised increases, people need to be confident in the security of their privacy. It is essential that the law support this with robust provisions.

Emerging online business models adopt methods based on slogans like "ask forgiveness, not permission",[1] "move fast and break things",[2] or other variants which in effect de-emphasize consent and avoid responsibility. In the digital environment, there are often high levels of risk-taking and a cavalier approach to privacy and consent, rather than one based on accepting responsibility for pushing risks onto data subjects, and compliance with the letter and spirit of existing privacy protection law.

In our view, the proposed tort should include intentional and reckless behaviour and also gross negligence. Parties in receipt of private material ought to take responsibility to store, track and control that information. To support the level of confidence and security the digital era demands, people must be assured that their private information is safe. Excluding negligence entirely provides minimal incentive to put in place procedures to protect privacy. The inclusion of a "gross negligence" standard would provide such incentives, while avoiding liability for the "absent-minded

person" who "walks into a neighbour's home" (ALRC Discussion Paper 80 para [5.86]).

A gross negligence standard will increase the reach of the proposed tort. We feel this is important to avoid a negative spiral, a race to the bottom, where decreasing protection or enforcement of privacy leads to lower expectations, which in turn decreases the scope of the tort. A gross negligence standard will encourage particularly those with the means to do so to take responsibility for the protection of private information, in turn maintaining community expectations around privacy.

---

[1] Originally attributed to software pioneer Grace Hopper, *Chips Ahoy* magazine, US Navy, July 1986, http://www.chips.navy.mil/archives/86_jul/interview.html (via archive.org), widely used in software circles.

[2] See e.g. Mark Zuckerberg's letter to investors in Facebook's IPO, 'Mark Zuckerberg's Letter to Investors: 'The Hacker Way'', *Wired*, 1 February 2012, at: http://www.wired.com/2012/02/zuck-letter/

Proposal 5–3 :

N/A

Proposal 5–4 :

N/A

Proposal 6–1 :

We agree that the privacy tort should only be actionable in situations where a person had a reasonable expectation of privacy and, consistent with our comments on Proposal 5-2, would have expected that a reasonable person in the circumstances would adequately protect their privacy. In this respect it is essential to emphasise that people have a right to an expectation of privacy and that the law will support them in cases of serious breach of those expectations.

However, if aspects of the ALRC proposal which currently set the bar too high are not addressed, this "reasonable expectation" test potentially creates a perverse incentive to data users to pursue poor practices which in effect erode the expectation of privacy but fall just short of the scope of the tort.

It is vital therefore not to demand a standard of proof and fault elements which present such a barrier to potential litigation as to discourage legitimate claims from seeking redress. It is critical that while restricting action to the community's reasonable expectations (through proposal 6-1), the model for a tort supports a rigorously high standard for those expectations (through our recommended change to proposal 5-2) to prevent an erosion of privacy requirements.

To demand a reasonable expectation of privacy on the plaintiff's behalf while not similarly demanding a minimum duty of care on behalf of potential defendants invites a progressive degradation of privacy standards.

Proposal 6–2 :

We propose minor changes to the list of factors a court may consider.

First, delete the words "including any device or technology" as unnecessary and potentially divisive. The term "means used" seems sufficiently inclusive to cover all devices, software and other tools that may be used. The problem with including the word "technology" is that the definition of that term is often contentious – some treating it as synonymous with "means", others as including methods of governance and law, and others as a type of knowledge.

Secondly, change "whether the plaintiff consented to the conduct of the defendant" to "whether the plaintiff has consented to the conduct of the defendant and the nature of any such consent, taking account of its voluntariness, explicitness, severability and revocability and the adequacy of the information provided as to the ways in which the information will be used." Our suggestion takes account of the ALRC's comments on degrees of consent in (ALRC Discussion Paper 80 para [6.52]) without compromising the larger debate to which the ALRC referred.

Proposal 7–1 :

N/A

Proposal 7–2 :

N/A

Proposal 8–1 :

Public interest and freedom of expression should be confined to defences, and the public interest should be addressed by the defendant, it is not

appropriate to insist that the plaintiff has this additional hurdle embedded in the elements.

Reasons include:

- it represents ‘two bites at the cherry’, since there are already proposed a range of hurdles and defences which effectively reflect the need for balance
- establishing public interest as a balance to privacy breach should only occur after it is established such a breach has occurred, this puts the cart before the horse.
- the tort must emphasise the primary onus for establishing alternative public interest falls upon the defence to prove not upon the plaintiff to establish and it should thus be reserved as an defence.
- privacy itself is an essential public interest intrinsic to basic freedoms and civil rights. It is inappropriate to insist that plaintiff’s must determine to the court which fundamental rights they desire at the expense of others.

Proposal 8–2 :

Many broader public interests depend on strong protection of privacy, confidentiality and personal information security. Framing ‘broader public interests’ as opposed to privacy is to miscast privacy as an entirely private value, opposed to public interests and values.

There are a number of suggested factors are too broadly cast, and of insufficient gravity to warrant a serious invasion of a person’s privacy.

First the “proper administration of government” is too broad to defeat an otherwise non-litigable right. Proper administration should at its heart privilege key personal rights and interests such as privacy over mere administrative convenience.

Similarly “the economic well being of the country” is perversely broadly cast, and wrongly framed as a countervailing factor. Many aspects of online commerce rely on trustworthiness and confidence in privacy and information security. Economic vibrancy demands security of confidential business practice and should not be balanced against it.

Proposal 9–1 :

N/A

Question 9–1 :

N/A

Proposal 9–2 :

N/A

Proposal 9–3 :

The scope of private information available in the digital era and the potential for harm if it is used inappropriately is both widespread and far reaching.

The report considers those breaches of a serious nature which come with equally serious consequences. We wish to emphasise (1) the potential for breaches of privacy to be directly linked to a person's cause of death through a variety of means, and (2) an increasing trend of harassment and defacement of on-line and off-line memorials which cause great distress and damage to families and loved ones.

The outrage caused by the public defacement of online memorials in the Trinity Bates murder[1] highlight the privacy tort as an additional or alternative avenue of legal redress. The suicide of Tyler Clementi in the US[2] after secretly filmed footage of him kissing another man was posted online further emphasises the scope and impact of privacy threats in the digital era.

For these reasons we consider it important that in line with earlier observations (ALRC Issues Paper 43 para [110]) that serious invasion of privacy action persist to the plaintiff's estate. Given the importance of securing privacy, we advocate for both action surviving death, and also a widening of potential loss award avenues to the estate. To reflect the nature of the threat, consequences and importance of privacy to which this proposed legislation aspires, we consider that this recognition is vital.

The report (ALRC Discussion Paper 80 para [7.40]) identifies the difficulty in measuring harm to personal dignity in traditional damage assessments. We support this, and go further to note that invasions of privacy can cause damage to individual and family dignity which can persist and even intensify following death. The dignity of the departed is an important community value and we advocate that proposed privacy tort legislation should reflect that. Attacks on privacy can, in the worst case, create harms which contribute to or result in death, and attacks upon the privacy of deceased persons may also continue to damage their reputation, dignity and greatly distress their loved ones. Privacy tort legislation in the digital era should reflect these factors and the community values which support them.

---

[1] http://www.theaustralian.com.au/news/nation/autopsy-to-reveal-how-trinity-leigh-bates-died/story-e6frg6nf-1225833519592

[2] http://www.abc.net.au/news/2010-10-02/gay-suicide-puts-focus-on-cyber-bullying/2282342

Proposal 9–4 :

The security of personal privacy in the digital era presents challenges to society and the law which demand a flexible and innovative approach to traditional practices. Personal information can be compromised for extended periods of time before this has a notable direct social impact, or a potential plaintiff becomes aware of any breach. Defendants have the ability to collect private information, store it, and then use it in a harmful fashion at a much later time, compromising the traditional effect of limitation periods.

In light of the potential for significant time passing between the actual invasion of privacy and its effects or harms, no limitation period should be attached to the initial invasion (Proposal 9-4[b]). The nature of personal information and its modern storage potential means that an actionable tort should commence from when the 'actual harm' is perceived (Proposal 9-4[a]). This would enable the plaintiff to explore their options adequately. While we acknowledge this does step away from current legislative provisions, we emphasise both the unique challenges and also the social importance of protecting personal privacy.

Proposal 9–5 :

N/A

Proposal 10–1 :

In the light of developments including the Snowden revelations about mass surveillance practices, this defence seems too broad. The scope of this defence must be qualified by elements of transparency, necessity, justification, effectiveness and proportionality to prevent the existence or perception of "Big Brother" government intrusion.[1] Lawful authority provisions must be subject to independent review.

Additionally laws of other countries should not apply extraterritorially in Australia or to Australians to defeat this cause of action.

---

[1] International Principles on the Application of Human Rights to Communications Surveillance, 10 July 2013 (adopted by over 400 civil society organisations) at: <https://en.necessaryandproportionate.org/text>; see also UN General Assembly Resolution 68/167, 'The Right to Privacy in the Digital Age,' A/RES/68/167, 21 January 2014, available from: <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>

Proposal 10–2 :

N/A

Proposal 10–3 :

N/A

Proposal 10–4 :

This proposal, transferred inappropriately from defamation legislation, is potentially very broad. For example, there is nothing in the wording to suggest that "duty" could not include a contractual duty voluntarily undertaken so that a private investigator might come under a "duty" to disclose. Additionally the potential broad interpretation of "social" and "moral" interest and duty is cause for concern. As a result, given the broad range of potential interests and duties, this proposal as currently worded would seem to provide an unjustifiably broad exception to limit liability.

The unwanted release of personal information into the wider community, and direct defamation of character particularly via the media, are superficially similar, but in practice they have significantly different consequences, and need different remedies. Balancing an individual's rights to their own undisturbed private life against a limited set of legal and social demands of our community is important, but we feel as this proposal stands it does not support this balance. In the case of serious breaches of privacy we feel its scope demands a different approach and either, no, or a substantially narrower definition of, qualified privilege. The defence of qualified privilege should thus be omitted entirely, or else carefully and very narrowly restricted.

Question 10–1 :

N/A

Proposal 10–5 :

N/A

Proposal 10–6 :

N/A

Question 10–2:

N/A

Proposal 10–7 :

Any “safe harbour” scheme should be strictly limited to require internet intermediaries to act quickly and to the satisfaction of the complainant to deal with material related to serious invasions of privacy posted by third parties.

Both giant global operators and local microbusinesses can in practice place many obstacles to a data subject taking ‘self help’ action against such intrusions, with unresponsive web forms, delays and disputes, and reluctance to act vigorously. Safe Harbor schemes in the US have often failed to require the sort of good practice expected by users, so the highest possible standards of compliance, speed and auditing should be conditions embedded in the scheme, with protection stripped automatically for failure to comply with reasonable requests for assistance.

This particularly applies to young people. Our colleagues at the National Children's and Youth Law Centre have reported frequently encountering difficulties in getting prompt and effective action in relation to online material that poses risks of serious intrusion on privacy for young people, especially if hosted in the Cloud or offshore. Operation in Australia and seeking the protection of any safe harbour regime should entail minimum standards of responsiveness, timeliness and compliance with reasonable requests.

The existence of a safe harbour defence should not operate to enable intermediaries to continue with “business as usual” if this involves failure to meet such standards. Refusal to take down material that is a serious invasion of privacy, or a lesser standard for young people, should put the intermediary beyond this defence.

However, it is also important to avoid unnecessary take downs, so there should be a mechanism to establish a reasonable process or reasonable steps to assess the material or claim of required action, to apply reasonable criteria, and to offer a means for resolving disputes, perhaps using the TIO, which we have found in our report ‘Communications privacy complaints: in search of the right path’[1] to be relatively speedy and effective; or similar industry process, or the ACMA.

(See below for observations about the potential crossover with the ACMA takedown scheme.)

[1] 2010, http://cyberlawcentre.org/privacy/ACCAN_Complaints_Report/report.pdf (supported by ACCAN)

Question 10–3 :

N/A

Proposal 11-1:

N/A

Proposal 11–2 :

N/A

Proposal 11–3 :

N/A

Proposal 11–4 :

N/A

Proposal 11–5 :

N/A

Proposal 11–6 :

N/A

Proposal 11–7 :

N/A

Proposal 11–8 :

N/A

Proposal 11–9 :

N/A

Proposal 11–10 :

N/A

Proposal 11–11:

N/A

Proposal 11–12:

N/A

Proposal 11–13 :

N/A

Question 11–1 :

N/A

Proposal 12–1 :

N/A

Proposal 12–2 :

N/A

Proposal 13–1 :

We support in general proposals 13.1-4. We understand the Australian Privacy Foundation is addressing many of the issues in this area in some depth.

One reservation on surveillance device laws is that they limit the possibility of individuals recording illegal or wrongful behaviour eg corruption, bullying etc unless attached to the police (eg warrant) or newspaper (journalist exemption).

Proposal 13–2 :

The "technology neutral" idea for surveillance device is a good one in principle, but also needs to distinguish between very different technologies, eg drones with cameras and data surveillance by software, to the extent they raise different issues. In practice such neutrality is difficult to achieve, and may omit or overlook some of the potential for new or divergent technology to raise particular issues not considered previously.

For instance, surveillance devices will increasingly generate metadata not content, and they will increasingly be attached to the body and generate information about biological, locational and other attributes, not just the

traditional surveillance device outputs. The relevance of metadata as surveillance, and of the full range of data types collectible by such devices, should be encompassed.

Proposal 13–3 :

N/A

Proposal 13–4 :

N/A

Question 13–1 :

N/A

Proposal 13–5 :

N/A

Question 13–2 :

N/A

Proposal 14–1 :

N/A

Proposal 15–1 :

N/A

Proposal 15–2 :

N/A

Question 15–1 :

N/A

Question 15–2 :

This question is quite technologically specific, in that it is confined to a "website or online service". Why not a requirement to take down something off a billboard, or other service?

There should be equivalent means of requiring prompt removal or takedown for forms of technology and publication other than online and web services, using an appropriate means for each such forum.

It would also be preferable to integrate this web-centric proposal with the proposed "safe harbour" scheme above, as compliance with the take down scheme here could be mandated as one of the conditions on such a scheme, to reduce the prospect of abuse.

There should be investigation of the best way of bringing offshore online operators dealing in Australia into the scope of this requirement, as these will often be the main hosts. A requirement of the proposed safe harbour scheme for offshore operators to accept the authority of the ACMA in such disputes may be one means, although our *Drowning in Codes* report[1] raises concerns about the responsiveness of industry codes for consumers.

---

[1] Connolly and Vaile, "Drowning in Codes of Conduct: An analysis of codes of conduct applying to online activity in Australia" 2012, supported by auDA, http://cyberlawcentre.org/onlinecodes/

Proposal 15–3 :

N/A

Other comments:

No other comments

File 1:
File 2: