AMTA
Australian Mobile Telecommunications Association

COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

Australian Law Reform Commission
Serious Invasions of Privacy in the Digital Era

Submission
prepared by:

Australian Mobile Telecommunications Association and Communications Alliance Ltd

May 2014

Introduction

The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance Ltd (the Associations) welcome the opportunity to provide this submission in response to the Australian Law Reform Commission's (ALRC) Discussion Paper 'Serious Invasions of Privacy in the Digital Era' (the Discussion Paper).

The Associations wish to make clear up-front that we take very seriously the protection of personal information. However, we must also express our opposition to the proposal to introduce a statutory cause of action for serious invasions of privacy (privacy tort).

We do not consider that a case has been made for the introduction of such a tort, noting that there is already a range of laws in place to protect the privacy of individuals and which address the same issues to which the proposed new tort is directed. Moreover, there has not yet been time to consider the impact of recent *Privacy Act* reforms.

The Associations are concerned that a privacy tort would impose additional compliance costs on business while not providing any material benefit for members of the public. We believe the proposal is clearly contrary to the commonwealth government's red tape reduction program; and note the government is on the record opposing a privacy tort.

This submission explores in detail the matters outlined above. It also provides our views on some other measures raised in the Discussion Paper, specifically those related to surveillance; a proposed new privacy principle for the deletion of personal information; and a proposed new statutory tort of harassment.

Please note that Communications Alliance member Foxtel has not contributed to this submission and the submission does not represent its views.

The Associations

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

Introduction of a Statutory Cause of Action for Serious Invasions of Privacy

The Associations are strongly opposed to the proposal to introduce a statutory cause of action for serious invasions of privacy (privacy tort).

> *"Proposal 4-1: A statutory cause of action for serious invasion of privacy should be contained in a new Commonwealth Act*
> *Proposal 4-2: The cause of action should be described in the new Act as an action in tort"*.

The Associations do not consider that the case has been made for the introduction of a privacy tort.

While there is no established common law right of action in Australia for intrusion upon an individual's seclusion or private affairs, there is a range of laws which are designed or can operate to protect the privacy of individuals and address the same issues towards which the proposed new tort are directed. The handling of personal information (including sensitive information) is regulated by Commonwealth and State-based legislation. Various types of physical invasions of privacy can be protected by common law torts, such as trespass, the tort of nuisance and defamation, as well as actions for breach of confidence. There is also legislation in each State and Territory governing the use of surveillance devices.

The *Telecommunications Interception and Access Act 1979* also covers the legal interception of telecommunications services and the Associations note that this legislation is currently the subject of review by the Senate's Legal and Constitutional Affairs References Committee. This legislation also balances the privacy concerns of citizens with legal interception obligations on telecommunications providers. It is important for industry that any privacy obligations are clear and consistent with regulatory requirements around legal interception.

However, the ALRC has suggested that there are gaps and deficiencies in the existing legal framework and that a new statutory tort for serious invasions of privacy is necessary to fill such gaps. It is our strong view that any perceived deficiency in the current regulatory regime should not be addressed through the enactment of the privacy tort and that legal protections already exist which could be, if demonstrated to be necessary, amended to enhance privacy protection. We oppose the introduction of further privacy reforms without time and proper consideration being given to the impact of the recent *Privacy Act* reforms.

Government has expressed reservations

We also note that the Government has expressed reservations with regard to the introduction of a privacy tort. According to *The Australian*, Attorney-General Brandis has stated that:

> *"[T]he government has made it clear on numerous occasions that it does not support a tort of privacy".*[1]

Government De-Regulation Agenda

[1] Merritt, C., 'Brandis Rejects privacy tort call', *The Australian*, 4 April 2014, http://www.theaustralian.com.au/business/legal-affairs/brandis-rejects-privacy-tort-call/story-e6frg97x-1226873913819

The Associations consider that the introduction of a privacy tort will serve to create additional compliance costs for business without providing material benefit to the public. The introduction of new compliance requirements directly contradicts the intentions of the Government's red tape reduction program.

As noted in comments by the Hon. Josh Frydenberg MP, Parliamentary Secretary to the Prime Minister:

> *"This scandalous culture of piling on new regulations without assessing the consequences for productivity, and the costs involved, must now come to an end. We need a new approach. Questions must be asked first before new regulations are passed. What is their purpose? What is their cost? What is their impact on productivity? What is their impact on new entrants? And what is their effectiveness in managing risk? Only then, when it is absolutely necessary and with no sensible alternatives available, should we proceed to regulate. We need a new conception of acceptable risk and we need to much better understand the cumulative impact of regulation on business decision making."*

In summary, the Associations do not support the enactment of a privacy tort – with the associated increased compliance costs for business when legal protections already exist which, if demonstrated to be deficient, could be amended to enhance privacy protection.

Legal Design of a Statutory Cause of Action

Without detracting from our core position that the introduction of a privacy tort is unnecessary, we provide the following comments on aspects of the legal design of the privacy tort canvassed in the Discussion Paper.

Safe Harbour

In relation to the introduction of a safe harbour, the Discussion Paper states:

> *Proposal 10-7 the new Act should provide a safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their service*
>
> *Question 10-3 What conditions should internet intermediaries be required to meet in order to rely on this safe harbour scheme?*

While the Associations are supportive of the principle that a 'safe harbour' should be provided to protect internet intermediaries from liability, it is our strong view that there should not be any conditions attached to this protection.

In this context, internet intermediaries includes search engines, communication conduits such as ISPs, and online content hosts such as services like YouTube, eBay, Amazon, Facebook and Twitter. As is well understood, the speed at which content is generated makes it impossible for internet intermediaries to take down user-generated content, let alone ensure it is permanently removed and not re-published by the originator or others. The way in which the internet – and social media – is regulated (or not) is the subject of ongoing debate.

The Associations' concern is that the default position of some stakeholders is to seek to impose obligations on internet intermediaries, including ISPs and CSPs who provide the underlying connection, to take down content and/or terminate subscribers' accounts. That is, instead of tackling the originators of the content in issue, ISPs and CSPs may be burdened with additional regulation because it is perceived as too difficult or costly to pursue those who actually create the content giving rise to concerns. This provides no justification for placing obligations on internet intermediaries.

The problem with targeting internet intermediaries in order to regulate content can be summarised as follows:

> *"Intermediaries are what carry, store, and serve every speck of information that makes up the Internet….*
> *And yet, if we're not careful, we can easily lose all the benefits these intermediaries bring us. ..*
> *…by relieving intermediaries of liability for the content passing through their systems it has allowed for much more, and much more diverse, content to take root on them than there would have been had intermediaries felt it necessary to police every byte that passed through their systems out of the fear that if they didn't, and the wrong bit got through, an expensive lawsuit could be just around the corner. Because of that fear, even if those bits and bytes did not actually comprise anything illegal intermediaries would still be tempted to over-censor or even outright prohibit scads of content, no matter how valuable that content might actually be."*[2]

This is even more complex if internet intermediaries are expected to make judgments regarding whether an invasion of privacy may have taken place. It is not appropriate to expect that internet intermediaries be responsible for making nuanced legal judgements with regard to whether an invasion of privacy may or may not have occurred.

Placing an obligation on internet intermediaries to take down content before any due process has taken place is also bound to lead to the removal of legitimate speech. Internet intermediaries should not be required to remove material that may invade a person's privacy unless given appropriate notice, such as by a court.

The ALRC has considered safe harbour regimes in overseas jurisdictions, in particular Section 230 of the *Communications Decency Act 1996 (US)*. The Discussion Paper states:

> *"10.71 Arguably, section 230 provides too much protection from liability. As discussed below, it may be appropriate to require internet intermediaries to take reasonable steps to remove material that invades a person's privacy when given notice. This might be a condition of relying on a safe harbour scheme".*

The Associations strongly oppose this view. Section 230 does not provide 'too much protection' from liability. Rather, it recognises the unique role that internet intermediaries play and affords them appropriate protection from liability. The stated policy underlying s230 of the *Communications Decency Act* included a perceived need to "preserve the vibrant and competitive free market" in Internet service provision.

Also, the Associations do not support the view expressed that 'a safe harbour scheme may not be necessary if, as the ALRC proposes, the new tort is only actionable where the defendant has intentionally or recklessly invaded the privacy of the plaintiff'. (para 10.75 of Discussion Paper).

[2] Gellis, C, 'Protecting Internet Intermediaries', http://www.project-disco.org/intellectual-property/021814-protecting-internet-intermediaries/

An internet intermediary that does no more than facilitate the dissemination of content that may invade privacy should be deemed not to be a publisher of that matter, whether or not the intermediary is on notice of the allegedly privacy invasive matter.

The Associations consider that attaching conditions to any safe harbour protection has the potential to undermine the protection it is seeking to afford. Any safe harbour for online intermediaries must be clear and robust to ensure that protection is meaningful to ensure that internet intermediaries have certainty to continue their legitimate online operations, innovations and investment.

Other Measures to Improve the Protection of Privacy

Surveillance

The ALRC Discussion Paper also recommends the introduction of uniform surveillance device laws throughout Australia that include a technology neutral definition of 'surveillance' device.

> *Proposal 13-1 Surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.*
>
> *Question 13-1 Should the states and territories enact uniform surveillance laws or should the Commonwealth legislate to cover the field?*

The Associations agree with the ALRC that the present lack of uniformity across state-based legislation results in increased *'uncertainty and compliance burdens for organisations'*. As such, the Associations support the introduction of consistent legislation. It is our view that this complexity could be reduced through the introduction of a Commonwealth law.

A New Privacy Principle for deletion of personal information

The ALRC received submissions arguing that the harm caused by a serious invasion of privacy could be augmented by the endurance of private data in the public sphere. The ALRC proposes:

> *Proposal 15-2 A new Australian Privacy Principle should be inserted into the Privacy Act 1988 (Cth) that would:*
>
> *(a) Require an APP entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual; and*
>
> *(b) Require an APP entity to take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance*

The Associations are strongly opposed to the introduction of a new Australian Privacy Principle (APP) relating to the destruction or de-identification of personal information given the rights already conferred by the existing APPs.

The proposed requirement would require an entity to make an assessment of what information falls within the definition of 'personal information' to determine what has to be

removed. This assessment is not always straightforward, particularly where there could be information connected with the personal information to be removed that is not covered by the removal obligation.

Currently, an APP entity is required to *'take such steps as are reasonable in the circumstances'* to destroy or de-identify personal information if the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity in accordance with the APPs.

Further, a customer of an APP entity, such as an ISP, already has the right to request correction of their personal information under the APPs. Telecommunications companies endeavour to keep personal information up-to-date. The Associations contend that consumers need to work with providers to update their own their own personal details where appropriate. It would concern the industry if the work done to empower customers to support this joint responsibility was not recognised or eroded by the introduction of a new APP.

The proposal to insert a new APP that extends current obligations of correction of personal information is impractical.

The Discussion Paper also includes a section that considers the need to empower a regulator, such as the Australian Communications and Media Authority, to order an organisation to remove information.

> *Question 15-2 Should a regulator be empowered to order an organisation to remove private information about an individual, whether provided by that individual or a third party, from a website or online service controlled by that organisation where:*
>
> *(a) The individual makes a request to the regulator to exercise its power;*
>
> *(b) The individual has made a request to the organisation and the request has been rejected or has not been responded to within a reasonable time; and*
>
> *(c) The regulator considers that the posting of the information constitutes a serious invasion of privacy, having regard to freedom of expression and other public interests?*

The Associations are strongly opposed to the introduction of a regulator take-down system for serious invasions of privacy. Considering the speed and volume of user generated content is created and published via social media the implementation of such as system is likely to be impossible to comply with and costly and time-consuming for government and business, as well as being ineffective in relation to user-generated content (for reasons discussed above). Additionally, and as the ALRC itself has noted, such a system '*may have an undesirably chilling effect on online freedom of expression'*.

New Tort for Harassment

The ALRC proposes the enactment of a Commonwealth statute which provides for a new statutory tort of harassment, and which makes existing criminal offences for harassment uniform across the country.

As outlined above, the Associations consider that existing privacy framework to be adequate. As such, we are also sceptical that there is merit in enacting a new statutory tort of harassment.