SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA
(Australian Privacy Foundation Submission to the Australian Law Reform Commission)

15 November 2013

Authors[*]

Bruce Arnold, Assistant Professor in Law, University of Canberra
David Lindsay, Associate Professor of Law, Monash University
Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales
David Vaile, Co-Convener, Cyberspace Law & Policy Community, UNSW
Nigel Waters, Pacific Privacy P/L
Roger Clarke XamaX Consultancy P/L

Abstract

This submission by the Australian Privacy Foundation (APF) to the Australian Law Reform Commission (ALRC) strongly endorses establishment in national legislation of a cause of action for serious invasion of an individual's privacy which, for convenience, this submission shall generally refer to as a statutory tort. The submission answers the 27 questions asked by the ALRC in its October 2013 Issues Paper 'Serious Invasions of Privacy in the Digital Era'.

Such a tort has been recommended by a succession of law reform commissions and other bodies. Recurrent recommendation demonstrates that there is a substantive and significant need for the tort and that after wide consultation those bodies consider that legislation is both desirable and viable. The tort has not been ruled out by the High Court and could be accommodated under the national constitution. As noted by the law reform commissions the tort will not inhibit effective law enforcement or national security activity. It will not inhibit the implied freedom of political communication, a freedom that the High Court and Supreme Courts have indicated is not absolute. There is no reason to believe that the tort will burden the legal system with inappropriate litigation. Criticisms of the tort are exaggerated and typically reflect vested interests.

Fundamentally, the tort offers an effective remedy for problems that are evident in Australian law, that are of concern to many Australians, and that have been acknowledged by both courts and law reform bodies over a considerable period of time. The tort will provide coherence across the Australian jurisdictions, where there is major inconsistency including, for example, in surveillance devices legislation. The tort will also offset regulatory incapacity, in particular the very restricted scope of the *Privacy Act 1988* (Cth) – concerned with information privacy – and under-resourcing of the Office of the Australian Information Commissioner (OAIC). It will fill a long-standing gap in the common law protection of the right to privacy, which is not adequately covered by existing causes of action. The Foundation further considers that an important role of the tort is in signalling to all Australians that privacy should be respected as a matter of rights and obligations; that 'signalling' function is likely to be as significant as any deterrent associated with damages under the tort.

[*] The authors are the principal drafters of this submission on behalf of the Australian Privacy Foundation (APF). We wish to thank all other members of the APF's Board,

Australian Privacy Foundation

w e bsite : w w w . p r i v a c y . o r g . a u

SUBMISSION TO ALRC ISSUES PAPER: *SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA*

Professor Barbara McDonald
Australian Law Reform Commission
Sydney

Dear Professor McDonald

The Australian Privacy Foundation welcomes the Australian Law Reform Commission's consultation regarding privacy. This document responds to the Commission's call in October 2013 for public comment on its 'Serious Invasions of Privacy in the Digital Era' Issues Paper.

The following paragraphs provide a background and overview before addressing specific questions in the Issues Paper. The Foundation would be happy to address any point in more detail.

The Australian Privacy Foundation

The Foundation is Australia's leading civil society organisation concerned with privacy. Its board includes legal practitioners, academics and information technology specialists. It has been an active contributor to national and state/territory privacy policy development over many years. It has a particular interest in the interaction of new technologies and social activity with privacy, data protection and confidentiality.

The Foundation operates on an apolitical basis.

In contributing to policy development the Foundation emphasises principles (for example as productive of regulatory coherence and respect for all Australians). It seeks to situate law enforcement, commercial and other activity within a principles-based legal framework.

In doing so it recognises the importance of law enforcement and problems that arise where public administration is based on bureaucratic convenience rather than a respect for the human rights and responsibilities highlighted by the ALRC in the consultation paper. Recognition of privacy is wholly consistent with good government, economic growth, a vibrant media and personal flourishing.

Summary

The Foundation strongly endorses establishment in national legislation of a cause of action for serious invasion of an individual's privacy which, for convenience, this submission shall generally refer to as a statutory tort.[1]

That tort has been recommended by a succession of law reform commissions and other bodies. Recurrent recommendation demonstrates that there is a substantive and significant need for the tort and that after wide consultation those bodies consider that legislation is both desirable and viable. The tort has not been ruled out by the High Court and could be accommodated under the national constitution.

As noted by the law reform commissions the tort will not inhibit effective law enforcement or national security activity. It will not inhibit the implied freedom of political communication, a freedom that the High Court and Supreme Courts have indicated is not absolute. There is no reason to believe that the tort will burden the legal system with inappropriate litigation.

The tort will provide coherence across the Australian jurisdictions, where there is major inconsistency including, for example, in surveillance devices legislation. The tort will also offset regulatory incapacity, in particular the very restricted scope of the *Privacy Act 1988* (Cth) – concerned with information privacy – and under-resourcing of the Office of the Australian Information Commissioner (OAIC). It will fill a long-standing gap in the common law protection of the right to privacy, which is not adequately covered by existing causes of action.[2] The Foundation further considers that an important role of the tort is in signalling to all Australians that privacy should be respected as a matter of rights and obligations; that 'signalling' function is likely to be as significant as any deterrent associated with damages under the tort.

Fundamentally, the tort offers an effective remedy for problems that are evident in Australian law, that are of concern to many Australians, and that have been acknowledged by both courts and law reform bodies over a considerable period of time. Criticisms of the tort are exaggerated and typically reflect vested interests.

Principles

The Foundation endorses the following principles identified by the ALRC:

- recognition of privacy as important for individuals to live a dignified, fulfilling and autonomous life;
- substantive public interest in the protection of individual privacy and confidentiality;
- the balancing of privacy with other values and interests, including the promotion of open justice, freedom of speech, the protection of vulnerable persons and national security and safety;
- consistency with international standards and obligations in privacy law;
- flexibility, adaptability and certainty in application and interpretation;
- coherence and consistency in the law applying throughout Australian jurisdictions;

[1] The APF recognises the debate concerning whether or not the statutory cause of action is properly classified as a 'tort', but does not address this issue in this submission: see, for example, NSW Law Reform Commission, *Invasion of Privacy* (Report 120), April 2009, pp. 41-3.
[2] D. Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339.

- access to justice for those affected by serious invasions of privacy.

Those principles are reflected in the Foundation's responses to the questions posed by the ALRC in the 2013 Issues Paper, as follows.

Question 1: What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

The Foundation endorses the above principles in aggregate and considers that they should be interpreted and applied on a holistic basis. Privileging one attribute – such as convenience in the enforcement of civil or criminal law – over principles results in law and practice that lacks legitimacy and coherence. In moving beyond the current consultation paper the ALRC should resist suggestions to 'stack' rights in a hierarchy and accordingly, for example, privilege the interests of commercial broadcasters, connectivity providers and social network services or law enforcement personnel.

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. In the Foundation's view, a private right of action in the form of a statutory tort is the long-needed essential counterpart of the existing regulatory framework, one which promises 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 more rapidly evolving technologies

That said, Australian jurisprudence over the past forty years has demonstrated that courts are capable of dealing with tensions in the interpretation of public and private interest, for example regarding defamation, national security and confidentiality. Consistent with the reports of the Victorian Law Reform Commission, New South Wales Law Reform Commission and the ALRC itself the Foundation encourages the Commission to question hyperbole by representatives of vested interests who claim that establishment of the tort would cripple law enforcement, damage the implied freedom of political communication, erode Australia's national competitiveness or serve as a refuge for the guilty.

Question 2: What specific types of activities should a statutory cause of action for serious invasion of privacy prevent or redress? The ALRC is particularly interested in examples of activities that the law may not already adequately prevent or redress.

Private causes of action for the protection of privacy in common law jurisdictions draw upon the four privacy torts first identified by William Prosser, and subsequently codified in the US *Second Restatement of the Law of Torts*.[3] The four torts are:

- unreasonable intrusion upon the seclusion of another;
- appropriation of another person's name or likeness;
- unreasonable publicity given to another person's private life; and
- publicity that unreasonably places another person in a false light before the public.

Of these, the first and third torts are most closely related to protection of the right to privacy, with the second and third torts extending to protect interests in addition to privacy, such as commercial interests in an image or reputation.

[3] William Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

The Foundation considers that the rights and interests falling within the Prosser taxonomy are not adequately protected under current Australian law. As pointed out in the 2009 NSW Law Reform Commission Report, there are clear gaps in the protection of privacy under existing private law causes of action, including:

- uncertainty concerning whether or not the equitable action for breach of confidence is available where private information has been not obtained in circumstances importing a duty of confidentiality;
- the limitations in the action for intentional infliction of emotional harm, which prevent it from applying to intrusions that do not cause recognisable psychiatric harm; and
- the lack of actionability of intrusions, such as those at issue in *Kaye v Robertson,*[4] where unauthorised photographs were taken of a television personality lying injured in a hospital bed.

Moreover, the emergence of new technologies and applications, including drones and wearable devices, such as Google Glass, highlight and exacerbate the existing gaps in the law. It is likely, for example, that 'passive' monitoring by drones or wearable devices fall outside the parameters of existing causes of action, but nevertheless pose privacy risks that should be addressed.

Question 3: What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?

Consistent with the preceding comments, the Foundation advises against specifying activities that should be privileged by the Act. That advice does not mean that appropriate and proportionate law enforcement action should breach the cause of action. (As noted above the Foundation urges the ALRC to look critically at claims that the tort will have deleterious effects, claims that were made when the *Privacy Act 1988* (Cth) and state/territory privacy statutes were introduced and have been shown to be unfounded.)

In considering what is 'unduly' restrictive the Foundation notes weaknesses within the *Privacy Act 1988* (Cth) and other legislation that feature substantial formal 'carve-outs' and that are further undermined by incapacity (lack of power, resources and will) on the part of regulators such as the Commonwealth Privacy Commissioner (as part of the OAIC). It is highly undesirable that the scope for action regarding serious invasions of privacy be seriously eroded through major exemptions or by limiting the ability to bring an action by a regulator, such as the OAIC.

Question 4: Should an Act that provides for a cause of action for serious invasion of privacy (the Act) include a list of examples of invasions of privacy that may fall within the cause of action? If so, what should the list include?

Inclusion of a list of examples may be useful in guiding courts and more broadly in addressing unfounded anxieties about the purpose of the legislation or its scope. Inclusion of examples in the statute rather than merely in extrinsic aids to interpretation such as the Explanatory Memorandum and 2nd Reading Speech is not remarkable or inconsistent with Australian drafting practice.

The Foundation considers that the list should be clearly identified as non-exclusive and

[4] [1991] FSR 62.

non-exhaustive, ie courts should be able to deal with serious invasions of privacy that fall outside the list. This should be made abundantly clear in the legislation itself, as well as in any extrinsic material, so as to prevent the courts from adopting an overly-restrictive interpretation of any illustrative list. This approach is consistent with the Foundation's endorsement of flexibility as one of the principles underlying the Act.

Question 5: What, if any, benefit would there be in enacting separate causes of action for: misuse of private information; and intrusion upon seclusion?

The three Australian law reform commissions that have recommended enacting a private cause of action have adopted different approaches to the design of the cause of action. While the ALRC and the NSWLRC supported a single cause of action, the VLRC favoured two causes of action, broadly corresponding to Prosser's intrusion and publication torts.

The main disadvantage of separate causes of action is that they may be under-inclusive. The introduction of two causes of action for intrusion and publication may, for instance, result in some identifiable privacy breaches not being covered by either tort. In particular, there might be occasions where personal information is accessed and used, without there being any actionable intrusion or publication. The Foundation supports a single cause of action, as an appropriately drafted cause of action will prevent privacy harms from 'falling through the cracks'.

While separate causes of action can promote certainty and flexibility by, for example, allowing for defences to be specifically tailored, the Foundation considers that it is possible to achieve this within a single cause of action.

Question 6: What should be the test for actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?

Consistent with the principles noted above the Foundation considers that actionability should depend mainly on the identification of circumstances where there is a reasonable expectation of privacy. This is an objective test that also provides flexibility, and which can be interpreted by the courts to reflect both principles and evolving social practice.

In any event, a 'serious' invasion should not be predicated on identifiable psychiatric harm or other specific harm to the individual whose privacy has been invaded as, in the first instance, actionability should be addressing the invasion rather than the harm. The severity of the harm is a matter that is appropriately taken into account in determining remedies.

Regarding the invasion itself, the Foundation considers that the threshold for actionability should be left largely to the courts. In this respect, the Foundation considers that a requirement for the invasion to be 'serious' should provide a sufficient safeguard against trivial complaints, without the need for a more detailed test. A threshold based on the 'seriousness' of the invasion or breach should be sufficient to avoid the tort being so wide as to allow for actions by persons who are merely offended or embarrassed.

Question 7: How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that: competing public interests must be considered when determining whether there has been a serious invasion of privacy; or public interest is a defence to the statutory cause of action?

The Foundation considers that this matter can be addressed through reference in the Act to a requirement that public interest be considered by courts in dealing with action for serious invasion of privacy. That consideration should be undertaken on a holistic basis, ie not in a way that necessarily prioritises law enforcement or the implied freedom of political communication or the commercial media over respect for the individual whose privacy has been invaded.

The Foundation notes that Australian courts have successfully grappled with competing claims of public interest, in particular regarding publication by media organisations such as John Fairfax and the Australian Broadcasting Corporation. Public interest should be a defence to the statutory cause of action but that interest must be recognised in terms of public good rather than in terms of public curiosity, media group ratings or bureaucratic convenience.

Upon analogy with the tort of defamation and the action for breach of confidence, the balance between the public interest in protecting the right to privacy and other rights and interests (including rights to freedom of expression) is best undertaken by including public interest as an affirmative defence, rather than as a balancing exercise undertaken within the parameters of the cause of action. One reason for this is that a defendant will usually be best placed to lead evidence relevant to whether or not a privacy breach is in the public interest. Moreover, adequate recognition of the right to privacy suggests that the onus of establishing that there is a public interest in a breach should lie with defendants.

Question 8: What guidance, if any, should the Act provide on the meaning of 'public interest'?

The Foundation considers that there are real dangers in attempting to compile a 'shopping list' of issues that may fall within a public interest defence. One of the dangers is that attempting to construct a list can open the door to special pleading by private interest groups. If it is considered that some illustrative examples may assist the courts in applying a public interest defence, this can always be addressed in extrinsic materials.

The main problem with a public interest defence is the potential for it to be interpreted in a way that undermines the right to privacy. This has clearly occurred in the United States where, due to the influence of the First Amendment, the 'newsworthiness' defence has effectively trumped the public disclosure tort. As the Foundation regards privacy as a fundamental right, the preferred approach is to require that all defences comply with the principle of proportionality. In the event that the proportionality principle is not adopted, some consideration could be given to limiting the defence to matters of 'legitimate public concern', as suggested by Gault P and Blanchard J in the New Zealand decision, *Hosking v Runting*.[5]

[5] [2005] 1 NZLR 1, 32.

Question 9: Should the cause of action be confined to intentional or reckless invasions of privacy, or should it also be available for negligent invasions of privacy?

The Foundation considers that the cause of action should encompass 'serious' invasions of privacy *per se* and should thus include negligent breaches. As noted above, concerns that the cause of action might encourage trivial or vexatious complaints can be dealt with by means of a threshold confining the action to 'serious' invasions or breaches.

Question 10: Should a statutory cause of action for serious invasion of privacy require proof of damage or be actionable *per se*?

The cause should be actionable *per se*. This approach best reflects the principles articulated by the ALRC. As a legal system we should be signalling that 'serious' invasion of privacy is abhorrent, irrespective of whether the subject of that invasion is highly resilient, is psychologically traumatised by the invasion or experiences financial injury.

Requiring proof of damage burdens potential litigants and is likely to deter some people from taking action over substantive invasions by well-funded parties. As explained in this submission, concerns that the cause of action may extend to everyday conduct that should not be actionable are best addressed by confining the action to 'serious' invasions or breaches.

Question 11: How should damage be defined for the purpose of a statutory cause of action for serious invasion of privacy? Should the definition of damage include emotional distress (not amounting to a recognised psychiatric illness)?

The action, and appropriate remedies, should be available where a person has suffered emotional distress, embarrassment or humiliation. Whenever there has been a 'serious' invasion of privacy, it should be possible for a complainant to obtain a remedy. The remedy must, of course, be proportional to the harm suffered.

Question 12: In any defence to a statutory cause of action that the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property, should there be a requirement that the act or conduct was proportionate, or necessary and reasonable?

Yes. Proportionality is an essential requirement, in relation to each and every defence.

The Foundation fully recognises and endorses the appropriateness of action by law enforcement and national security personnel, provided always that it is within an appropriate rights-based framework. The Foundation is, for example, on the public record as supporting instances where what would otherwise be regarded as invasive is legitimate and desirable in the public interest.

The Foundation cautions, however, about the danger of fundamentally weakening the tort through a 'carve-out' for particular interests. Given a majority in the relevant legislature it is a simple matter for a particular government to enact 'law and order' or 'national security' legislation that authorises representatives of the state to behave in

ways that raise legitimate and serious concerns regarding civil liberties. Those concerns can be best addressed through a requirement that the behaviour be proportionate, necessary and reasonable rather than based on what a particular agency or politician considers to be administratively convenient or electorally attractive.

Given an appropriate emphasis on rights-based principles, the Foundation considers that it is possible to identify a principled, context-specific balance on a case by case basis. In practice, the balance can be underpinned by a statutory requirement that, in order for the act or conduct to be justified it must be proportionate, necessary and reasonable.

Question 13: What, if any, defences similar to those to defamation should be available for a statutory cause of action for serious invasion of privacy?

As pointed out in the 2009 NSW Law Reform Commission report, defamation defences are not necessarily applicable to a privacy tort as privacy and defamation protect different interests.[6] For example, the defence of truth is clearly inapplicable to a privacy action. Moreover, some defamation defences – such as the defences of honest opinion and extended qualified privilege – would fall within a broad public interest defence.

The NSW Law Reform Commission proposed that that the following four 'defamation' defences should apply to a statutory cause of action for the protection of privacy:

- absolute privilege (for parliamentary and judicial proceedings);
- qualified privilege (for fair and accurate reports of proceedings of public concern);
- qualified privilege (duty/interest); and
- innocent dissemination.

As Butler explains, in a helpful table,[7] these defences are broadly analogous to defences to privacy torts under the US *Second Restatement*. While the first two of the above defences would likely be protected under a general public interest defence, the Foundation considers that specific defences may be justified as necessary to protect freedom of expression. The Foundation is, however, less convinced of the need to specifically include an analogue for the duty/interest form of qualified privilege, as this may best be dealt with under a public interest defence.

The Foundation considers that particularly difficult issues arise in relation to the liability of intermediaries, especially those involved in the dissemination of private material online. At this stage, the Foundation considers that the potential liability of intermediaries, including any form of accessorial liability, should be subject to further investigation, before any consideration is given to defences analogous to the defence of innocent dissemination. In this respect, the Foundation notes that the need for a defence of innocent dissemination arises as a result of strict liability for the publication of defamatory material. In circumstances where liability attaches to intermediaries, it may be appropriate to limit remedies where an intermediary complies with a prescribed procedure, such as a requirement to remove or 'take down' material.

[6] NSW Law Reform Commission, *Invasion of Privacy* (Report 120), April 2009, pp. 45.
[7] D. Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 385-6.

Question 14: What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?

The Foundation considers that, in general terms, an appropriately defined public interest defence is preferable to attempting to precisely define, in legislation, the circumstances in which privacy breaches may be justified. That assessment reflects the Foundation's emphasis on principle as noted above. The Foundation urges the ALRC to consider the tort on a holistic basis and to avoid a sectoral approach (ie by particular industry, medium or action) that risks rendering the tort incoherent or privileging particular interests over others.

Question 15: What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?

Provided the elements of the statutory cause of action, and defences, are appropriately defined, the Foundation does not see the need for exempting particular activities or types of activities.

Question 16: Should the Act provide for any or all of the following for a serious invasion of privacy: a maximum award of damages; a maximum award of damages for non-economic loss; exemplary damages; assessment of damages based on a calculation of a notional licence fee; an account of profits?

The Foundation considers that remedies should encompass damages (including exemplary damages), an account of profit, apology, retraction and injunction. The courts should be given sufficient flexibility to determine the most suitable remedies and, in this respect, the tort should be drafted in terms that do not unduly restrict the court's discretion.

Question 17: What, if any, specific provisions should the Act include as to matters a court must consider when determining whether to grant an injunction to protect an individual from a serious invasion of privacy? For example, should there be a provision requiring particular regard to be given to freedom of expression, as in s 12 of the *Human Rights Act 1998* (UK)?

Australian courts have not enshrined a broad, self-standing right to freedom of expression. This suggests that there may be some value in incorporating a provision such as s 12 of the *Human Rights Act 1998* (UK) in the statute, although the Foundation notes criticisms by figures such as Raymond Wacks in *Privacy & Media Freedom* (Oxford University Press, 2013). That said, considerations of 'prior restraint' must, in this context, appropriately take into account the extent to which privacy is uniquely vulnerable to any publication. Given this, it may be that freedom of expression is best addressed by means of the public interest defence.

Question 18: Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action? Who may bring a cause of action?

Apology and retraction should be included as non-monetary remedies, given that some subjects of serious invasion may not be interested in financial compensation. Apology has a valuable function in signalling acknowledgement of wrongdoing. So as to ensure proper redress, the remedies of apology and retraction should be complemented by a 'prominent publication' requirement.

Australian law provides for confidentiality in relation to corporations. Privacy as a human right should, however, be restricted to natural persons; there are alternate remedies for public/private organisations that may experience unauthorised access to and/or threatened/actual misuse of personal information. The action should not therefore be available to a corporate person in its own right.

Serious invasions should be actionable by a parent or guardian on behalf of those, especially minors, who lack legal capacity. The tort should also be actionable on a representative basis, given that multiple people may be the subject of a serious invasion by an organisation.

Question 19: Should a statutory cause of action for a serious invasion of privacy of a living person survive for the benefit of the estate? If so, should damages be limited to pecuniary losses suffered by the deceased person?

Given the Foundation's commitment to the protection of privacy as a fundamental right, the statutory tort should survive a deceased person, so as to allow for the appropriate vindication of that right post-mortem. As the introduction of a statutory tort will signal the unlawfulness of serious invasions, and as the courts can take the circumstances of a deceased person into account in awarding remedies, there is no need to limit remedies.

Question 20: Should the Privacy Commissioner, or some other independent body, be able to bring an action in respect of the serious invasion of privacy of an individual or individuals?

The Foundation is concerned that, given the costs of bringing an action before the courts, the introduction of a private cause of action, without more, may not adequately protect against serious invasions of privacy. Despite the Foundation's long-held concerns about regulatory failings in relation to the enforcement of complaints under the *Privacy Act 1988* (Cth), the Foundation supports giving the Commonwealth Privacy Commissioner the ability to bring 'own motion' actions before the courts for serious invasions of privacy. Over and above this, the Foundation considers that complainants should be given the option of pursuing a complaint for a serious invasion of privacy before the Privacy Commissioner. If a complainant is able to establish a breach of the statutory tort in proceedings before the Privacy Commissioner, this should amount to an 'interference of privacy', which would trigger the full enforcement regime under the *Privacy Act 1988* (Cth). Equipping the Privacy Commissioner with the power to address complaints of serious invasions of privacy will effectively supplement and reinforce the Commissioner's existing regulatory and enforcement functions. While complainants should have the option of bringing a complaint before the Privacy Commissioner, they should not thereby lose the right to bring an action before the courts. The proposed relationship between actions brought before the courts and complaints to the Privacy Commissioner is explained further in our response to Question 23.

Question 21: What limitation period should apply to a statutory cause of action for a serious invasion of privacy? When should the limitation period start?

Using the model of defamation action a one year period may be appropriate, with the limitation period starting from when the subject became aware of the invasion. Given increasing use of 'surveillance' technology that awareness may not arise until some time after the invasion has commenced or concluded.

Question 22: Should a statutory cause of action for serious invasion of privacy be located in Commonwealth legislation? If so, should it be located in the *Privacy Act 1988* (Cth) or in separate legislation?

For a coherent national regime it is essential that the cause of action be located in Commonwealth legislation. The Foundation considers that the Commonwealth has the constitutional power to introduce a uniform national regime.

If the Privacy Commissioner is to be given a regulatory role in receiving complaints for serious invasions of privacy, as is supported by the Foundation, the statutory tort should be introduced by appropriate amendments to the *Privacy Act 1988* (Cth). On the assumption that the existing enforcement regime under the *Privacy Act 1988* (Cth) should be available for serious invasions of privacy, incorporating the cause of action under the existing Act would simplify drafting. As explained elsewhere in this submission, it will also reinforce and extend the Privacy Commissioner's role as the regulatory agency responsible for dealing with privacy breaches.

Question 23: Which forums would be appropriate to hear a statutory cause of action for serious invasion of privacy?

The Foundation considers that private actions for breach of the statutory tort should be able to be brought before State and Territory Supreme Courts, the Federal Court of Australia and the Federal Circuit Court of Australia.

In addition, as explained elsewhere in this submission, the Foundation supports complainants being given the option of bringing a complaint relating to a breach of the statutory tort before the Privacy Commissioner. Such complaints should have the following features:

- If the Privacy Commissioner determines that there has been a breach of the statutory tort, this will constitute an 'interference with privacy', bringing all of the enforcement regime and remedies under the *Privacy Act 1988* (Cth) into play;
- At any time prior to a determination being made, the complainant should retain the option of bringing an action for a breach of the statutory tort before the courts;
- Both complainants and respondents should have a right to appeal from a determination of the Privacy Commissioner to the courts; and
- In such proceedings, findings of fact made by the Privacy Commissioner should be available to the court, consistent with the current provisions in the Act concerning enforcement of determinations, so that the matter does not need to be litigated *ab initio*.

Question 24: What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?

The Foundation recognises that some parties may wish to use alternative dispute resolution mechanisms, for example on the basis of cost, timeliness, stress or publicity. However, there should be no mandating of those mechanisms and in particular there should be no requirement for initial conciliation by the Privacy Commissioner. Of course, if both parties agree, they should have the option of conciliation under the *Privacy Act 1988* (Cth). As emphasised in this submission, the option of bringing a complaint under the procedures established under the *Privacy Act 1988* (Cth) should not prevent complainants from bringing an action before the courts.

Question 25: Should a person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation be permitted to bring or continue a claim based on the statutory cause of action?

The introduction of a private cause of action for the breach of privacy will provide private remedies where either none currently exist, or where existing legal protections are inadequate. The enforcement regimes under existing legislation - such as the Commonwealth, State and Territory information privacy laws – commonly have objectives additional to the vindication of a person's right to privacy. For example, Australia's information privacy laws are aimed, in part, at promoting good data management practices. Furthermore, the balances struck between the protection of the right to privacy and other rights and interests may differ, depending upon the particular legal regime. For example, the information privacy laws take into consideration the interests of government agencies and corporations in ways that may not be appropriate for a private cause of action. This suggests that a person who has received a ruling, or lodged a complaint, regarding a breach of privacy under existing laws should not be prevented from bringing a private action under a statutory cause of action. In this respect, it is important to bear in mind that the outcomes of complaints under existing statutory regimes can always be taken into account by the courts in the award of discretionary remedies.

No finding by the Privacy Commissioner in relation to any other interferences with privacy (including breaches of the APPs, credit reporting or TFN breaches, etc) should have any effect on the ability of a complainant to pursue a complaint or action concerning a serious interference of privacy pursuant to the statutory tort. The elements of the cause of action for the statutory tort are different from the elements of any other interference with privacy, so they must necessarily be decided independently of each other. However, where a court or the Privacy Commissioner has made findings of fact which are also relevant to a serious invasion of privacy, it should be possible for the court hearing that latter matter to take those findings of fact into account.

Question 26: If a stand-alone statutory cause of action for serious invasion of privacy is not enacted, should existing law be supplemented by legislation: providing for a cause of action for harassment; enabling courts to award compensation for mental or emotional distress in actions for breach of confidence; providing for a cause of action for intrusion into the personal activities or private affairs of an individual?

The Foundation considers that a statutory cause of action that is specifically designed to protect the right to privacy is preferable to both the current inadequate and piecemeal protection, and to the incremental development of other causes of action,

such as statutory recognition of an action for harassment or development of the equitable action for breach of confidence. While additional legislative recognition of the need to protect privacy would be welcome, the reference provides the ALRC with the opportunity to design a best practice, 'purpose specific' cause of action, rather than fiddling around the edges of existing actions.

Question 27: In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?

The title of the reference refers to 'the digital era' and, while there are many improvements that could be made to privacy protection in general, the following are suggested changes that are likely to have the most impact on serious invasions of privacy in the digital environment.

- ***Individuation not just identification.*** The definition of 'personal information' in the *Privacy Act 1988* (Cth) should be amended so that it no longer is restricted to information which has the capacity to identify an individual, but also includes information which provides the capacity (whether by itself or in conjunction with other information) for another entity to interact with an individual on an individualised or 'personal' basis. If an entity can send a person emails, SMS messages or the like, or configure their experience of a website or other digital facility, on the basis of information that depends upon their individual experience, history, preferences or other individuating factors, then such information should be regarded as personal information, and the interaction with them should be regarded as the use of such personal information. Such individuated/personalised interactions are now the basis of all marketing conducted on the Internet and via mobile telecommunications, and as such constitute one of most significant serious invasions of privacy in the digital era. Moreover, the Foundation considers that rapidly emerging marketing practices, including online behavioural advertising, psychographic profiling and predictive analytics, mean that this issue requires urgent attention. A change, along the lines suggested here, which is under consideration in current European law reform processes, would involve a major strengthening of privacy protection relevant to this reference.

- ***Re-identification*** The definition of 'personal information' in the *Privacy Act 1988* (Cth) should be amended so as to confirm that the information will remain personal information, despite any steps to anonymise it, if there is any significant possibility that it may be re-identified in future (or used for the purpose of individuated/personalised interactions, as described in the above proposal). This change would have a profound effect, on an 'industrial' scale, as a response to the challenges to privacy posed by so-called 'big data' and the techniques of data analytics/data mining. These techniques are the foundations of the personalisation of interactions, sometimes known as 'mass personalisation', and the identification and re-identification of individuals in the Internet/mobile communications environments. In addition, practices such as the increasing potential for metadata to be matched with other data to identify an individual's online behaviour currently fall largely outside the regulatory net. A reform such as this would, accordingly, also involve a major strengthening of privacy protection relevant to this reference.

- ***Data breach notification.*** A hallmark of the past decade has been a massive increase in large-scale data breaches or disclosures by both public sector and private sector organizations, mainly due to the capacity that the Internet has provided for both the disclosure of information (both inadvertently and via 'hacking' and other malfeasance) and its subsequent widespread and rapid dissemination. Therefore, a major strengthening of privacy protection relevant to this reference would result from the enactment of provisions for the prevention and notification of data breaches, as in the Bill which was not able to be enacted by the completion of the previous Parliament, but which received unanimous support from the Parliamentary Committee that considered it. Some aspects of that Bill could no doubt be improved, as the Privacy Foundation submitted in relation to the Bill, but it was also worthy of support as a matter of principle.

- ***Surveillance.*** A major concern for the Foundation has been an increase in the sophistication, intrusiveness and pervasiveness of surveillance technologies and practices. While a range of Commonwealth, State and Territory laws apply to surveillance devices and practices, the most significant laws are the State and Territory surveillance devices and listening devices Acts.[8]

  The State and Territory regimes are inconsistent, outdated and poorly enforced. Some of the problems with the regimes were identified by the Victorian Law Reform Commission in its 2010 report on *Surveillance in Public Places,* which concluded, in relation to the Victorian Act, that:[9]

  "At present the SDA [*Surveillance Devices Act 1999* (Vic)] regulates the use of surveillance devices inconsistently—certain activities are prohibited while others are effectively permitted because the Act says nothing about them. Furthermore, breaches of the Act attract serious criminal sanctions, which have proven not particularly effective in regulating public place surveillance".

The Foundation considers that the terms of reference provide an opportunity for the ALRC to review, and make recommendations for enhancing and improving, the inconsistent and inadequate State and Territory regimes that regulate surveillance technologies and practices. Given the present and emerging threats to privacy and individual liberties posed by surveillance devices and practices it is unacceptable for regulation to continue to be based on a patchwork of weak, technologically-outdated, poorly-known and poorly-enforced laws. In reviewing the State and Territory regimes, the Foundation considers that the ALRC should take into account:

- the desirability of introducing a uniform, Australia-wide regime, and the legal avenues available to the Commonwealth for promoting consistency among the State and Territories;
- the need to strengthen the State and Territory regimes so that, for example, they uniformly prohibit participant monitoring and appropriately restricting the extent to which 'implied consent' can be used to excuse unjustified surveillance, including covert surveillance;

[8] *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Listening and Surveillance Devices Act 1972* (SA); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).
[9] Victorian Law Reform Commission, *Surveillance in Public Places,* Final Report (May 2010), [6.109].

- the desirability of introducing civil penalties, which may go some way towards redressing the inadequate enforcement of the criminal offences established under the current regimes;
- the need for the legislation to be updated so as to effectively regulate new and emerging surveillance technologies; and
- in the absence of an effective regulator, the possibility of individuals bringing private actions to enforce breaches of surveillance devices laws.

The Foundation notes that submissions by individual members are likely to address further additional ways in which the current laws and regulatory frameworks are lacking and can be strengthened to better protect against serious invasions of privacy.

Question 28: In what other innovative ways may the law prevent serious invasions of privacy in the digital era?

The terms of reference require the ALRC to have regard to: "Innovative ways in which law may reduce serious invasions of privacy in the digital era". The Foundation considers that this provides the Commission with an opportunity to consider measures to address some of the most serious existing and emerging threats to the right to privacy, including threats that pose significant challenges to existing legal paradigms.

Protecting against serious invasions of privacy in a society that is increasingly characterised by the use of pervasive privacy-invasive and surveillance technologies, especially in the online context, cannot depend solely on law and regulation. There is a demonstrable need for holistic and concerted policies that promote education and privacy enhancing technologies, and incorporate appropriate assessment of privacy invasive technologies. All too often, government and regulatory responses to threats to privacy rights have been half-hearted, piecemeal and inconsistent.

Nevertheless, despite the limitations of legal solutions, laws can play a vital role in both inhibiting privacy invasions and in public education. An area of particular concern is the ready availability of affordable technologies that enable private individuals to collect, process and disseminate personal information on an industrial scale. This is particularly evident with the widespread use of social media, although it is not confined to those applications. The extent to which private individuals may increasingly engage in large-scale processing of personal information calls out for innovative legal and social strategies.

A first step in addressing these issues may be to focus on the right of individuals to delete personal information about them, such as photographs and videos, which has been posted online, especially to social media sites. This has become popularly known as the 'right to be forgotten'. As part of a fundamental review of the European Union data protection framework, the European Commission has adopted proposals for a new General Data Protection Regulation, which includes a version of a right to be forgotten.[10]

In its 2008 report on Australian privacy law, the ALRC rejected the view that the *Privacy Act 1988* (Cth) should be extended to apply to individuals acting in a non-

[10] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (Brussels, 25 January 2012) 2012/0011(COD), art. 17.

commercial capacity.[11] At that time, the Commission also rejected the possibility of establishing a take-down notice regime that would apply to online personal information.[12] Acknowledging that a statutory cause of action would not adequately address the problems arising from the use and disclosure of personal information on the Internet, the ALRC confined itself to emphasising the importance of public education, especially in relation to the 'privacy aspects of using social networking sites'.[13]

The Foundation notes that, since the ALRC's report, the use of social networking has become more pervasive and, accordingly, the privacy threats posed by social media have become more apparent. Moreover, it is only since 2008 that proposals for introducing a legal 'right to be forgotten' have received serious policy consideration, with proposed legislation now being under active consideration in the European Union. The problems are therefore much better understood, as are the undoubted complexities of attempting to draft laws that apply to social media.

In the light of these developments, the Foundation considers that the ALRC should revisit the conclusions reached in the 2008 report. In doing so, the Foundation believes that the current reference provides an opportunity for the ALRC to consider:

- the extent to which a 'right to be forgotten' should be incorporated under Australian law;
- the appropriate means for incorporating such a right, including the possibility of its incorporation in the *Privacy Act 1988* (Cth);
- if such a right were to be introduced, the appropriate scope of the right, including how rights to freedom of expression online can be best safeguarded; and
- the appropriate role of intermediaries, including social networking operators and search engine operators, in protecting online privacy.

In relation to serious invasions of privacy online, the Foundation considers that it is absolutely essential for the ALRC to give due consideration to the need for intermediaries, especially social networking service providers, but also search engine providers, to take appropriate responsibility for commercial services and activities which are premised on privacy invasions. This means that not only should the potential liability of intermediaries be considered in the context of innovative solutions to invasions of online privacy, but that full consideration should be given to the potential for intermediaries to be subject to secondary liability for breaches of any proposed statutory tort. If intermediaries were to be held secondarily liable for breaches of a statutory cause of action, the Foundation notes that there may be a case for a qualified defence that would limit liability where an intermediary takes reasonable steps to prevent privacy breaches, or limit the harms arising from online breaches.

The Foundation notes that submissions by individual members will address further means by which serious invasions may be addressed in the digital era.

[11] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008), [11.21].
[12] Ibid. [11.22]-[11.23].
[13] Ibid. [11.25].

For further information please contact:

David Lindsay david.lindsay@privacy.org.au

Board Member
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au