Professor Barbara McDonald
Australian Law Reform Commission
Level 40, MLC Tower
19 Martin Place
Sydney NSW 2000

Inquiry into Serious Invasions of Privacy

This submission responds to the October 2013 call by the Australian Law Reform Commission for public comment on the ALRC's 'Serious Invasions of Privacy in the Digital Era' consultation paper.

Summary

The following pages strongly endorse establishment in national legislation of a cause of action for serious invasion of an individual's privacy.

Establishment is consistent with recommendations by the Australian Law Reform Commission, NSW Law Reform Commission, Victorian Law Reform Commission and – most recently – the Law Reform Committee of the Victorian Parliament. It is not precluded by the national constitution. It is consistent with Australia's international agreements and is likely to be welcomed by Australia's courts.

Most importantly, access to effective remedies for egregious invasions of privacy reflects a respect for human dignity and autonomy that is fundamental to personal flourishing and justice in a liberal democratic state. Those remedies do not conflict with the freedom of political communication recognised by the High Court (or more broadly with free expression) and with law enforcement.

Australia's history of law reform – and the history of confidentiality law in the United Kingdom and other jurisdictions – indicates that hyperbole from self-interested critics about a flood of frivolous litigation or other ills should be vigorously questioned by the ALRC. In particular the Commission should be wary of claims made by representatives or associates of media organisations that have a history of privacy bad practice, a history demonstrated through current criminal proceedings against senior executives.

The Commission should also be wary of claims that privacy abuses can be (or indeed are being) effectively addressed by the Office of the Australian Information Commissioner, an entity that is concerned with information privacy. It regrettably lacks the technical expertise, funding and – most seriously – the will needed for effective action. The existence of a national watchdog, timid and toothless or otherwise, should not preclude private action. It is appropriate that individuals/classes who have experienced a serious invasion of privacy should have recourse to the courts for remedies that range from injunction to apology and damages. We should not expect or require a handful of Commonwealth officials to have sole responsibility and provide effective responsibility for all privacy abuses. We should also avoid development of an incoherent regime based on inconsistent recognition by state/territory courts of a tort that is specific to the particular jurisdiction.

The national parliament both can and should establish a national 'privacy tort' without delay. Establishment will be of benefit to all Australians.

Background

The submission is made by Bruce Baer Arnold.

Mr Arnold is an Assistant Professor, Law in the School of Law & Justice at the University of Canberra. Mr Arnold teaches Privacy & Confidentiality Law, Competition & Consumer Law and Intellectual Property Law. He is General Editor of the *Privacy Law Bulletin* practitioner journal and member of the Board of the Australian Privacy Foundation. He has written widely on privacy, data protection and confidentiality, including chapters in the LexisNexis *Privacy & Data Protection* service and work on privacy/confidentiality aspects of traditional knowledge. His writing has appeared in leading Australian and overseas journals, including *Melbourne University Law Review*. He has made invited submissions to a range of parliamentary and other inquiries.

The submission does not necessarily represent the views of the University of Canberra or other bodies such as the Australian Privacy Foundation. (The author contributed to and endorses the independent submission by the Australian Privacy Foundation.)

The following paragraphs do not involve what would be reasonably construed as a conflict of interest.

Basis

As the October ALRC paper recognises, the need for a statute-based national cause of action regarding serious invasions of privacy has been acknowledged by a succession of law reform bodies.[1]

That acknowledgment indicates that there are substantive reasons for establishment of a statutory tort, ie

- the Australian community, as demonstrated through recurrent official and nongovernment surveys, has indicated that privacy is important[2]
- serious invasions of privacy are occurring
- the existing patchwork of sectoral and technology-specific civil and criminal law (and data protection agencies)[3] provides inadequate redress for people who have experienced a serious invasion, an inadequacy exacerbated by the

[1] See Australian Law Reform Commission, *For Your Information: Australian Privacy Law & Practice* (ALRC Report 108, 2008); Victorian Law Reform Commission *Surveillance in Public Places — Final Report* (VicLRC report, 2010); New South Wales Law Reform Commission (2009) *Invasion of Privacy* (NSWLRC report 120, 2009); and Victorian Parliament Law Reform Committee, *Report of Inquiry into Sexting* (May 2013). See also New Zealand Law Reform Commission, *Privacy: Concepts & Issues, Review of the Law of Privacy* (NZLRC report, 2008).

[2] See for example the October 2013 Office of the Australian Information Commissioner 'Community Attitudes to Privacy' survey results, at oaic.gov.au.

[3] In preparing the ALRC's final report there would be value in identifying the mass of state/territory legislation that impinges on serious invasions of privacy, in particular to highlight major inconsistencies in law regarding official/private use of surveillance technologies and in law that potentially criminalises (and thereby deters/punishes) serious invasions but provides no scope for private action and compensation.

weakness of data protection agencies such as the Office of the Australian Information Commissioner[4]

- it is inappropriate to wait indefinitely for the High Court to be presented with a case that results in articulation of an Australia-wide common law tort and addresses the inconsistency apparent in decisions by the Queensland District Court, South Australian Supreme Court and Victorian County Court.[5]

Five objections are typically raised by interests opposed to a common law or statutory tort. Before considering the questions in the ALRC paper it may be worth reviewing those objections.

Claim 1: privacy is meaningless

It has been fashionable to claim that privacy is meaningless because it has been wholly eroded by digital technologies or that, in the words of one Australian academic, it is embraced by woolly minded members of the middle class who believe in santa claus and the tooth fairy or by people who have something to hide.[6]

That dismissal is inconsistent with

- the recognition of privacy as a right in a range of international agreements to which Australia is a party,[7]
- with statements by the High Court and the Supreme Courts, and
- with reference in privacy, crimes and other statutes to privacy as a value deserving of protection.

Claim 2: the tort is unnecessary

That claim is fallacious. The law reform commission reports and cases highlighted in the ALRC paper demonstrate that Australian privacy law and entities such as the OAIC are not effectively addressing serious invasions of privacy. That law is inconsistent: there is significant variation

- across the jurisdictions
- on the basis of types of information (eg health data),

---

[4] Ben Grubb, 'Long delays before privacy complaints assessed' *Sydney Morning Herald* (12 September 2013): "Australia's federal Privacy Commissioner has blamed the federal government for long delays in assessing breach-of-privacy and freedom-of-information complaints." As of November 2013 there are no indications that the OAIC will receive reinforcements and peer-reviewed publication based on information gained through the Freedom on Information Act might lead some observers to conclude that it has been captured by particular interests or lacks expertise in areas such as statistical analysis and genomics.

[5] *Grosse v Purvis* (2003) Aust Torts Reports 81-706; [2003] QDC 15; *Doe v Yahoo!7 Pty Ltd & Anor; Wright v Pagett and Ors* [2013] QDC 181; *Sands and State of South Australia* (2013) SASC 44; and *Doe v Australian Broadcasting Corporation & Ors* (2007) VCC 281

[6] Mirko Bagaric, 'Privacy is the last thing we need' *The Age* (22 April 2007). See also Mirko Bagaric, 'Rights must yield to community prosperity: the fallacy that is a strong right to privacy' in Brett Mason & Daniel Wood (eds), *Future proofing Australia: the right answers for our future* (Melbourne University Press, 2013) 65

[7] International human rights agreements referring to privacy (typically in terms of non-interference) include the 1948 *Universal Declaration of Human Rights* (UDHR) Art 12, the 1966 *International Covenant on Civil and Political Rights* (ICCPR) Art 17 and the United Nations 1989 *Convention on the Rights of the Child* (CROC) Art 16.

- on the basis of types of privacy (locational, information, integrity, otherwise)
- on the basis of the particular technology or
- on the use of that technology (eg whether a video camera has the sound turned on or off).

Claim 3: the tort will inappropriately chill free speech

The claim is typically being made by special interests and disregards the reality that in Australia there is no comprehensive right of free expression, as distinct from an implied freedom of political communication.[8]

There is no reason to believe that the tort, if established, will seriously inhibit legitimate investigative reporting, political commentary, documentary production or satire.

There is no reason to believe that it will "make it illegal to talk or write the truth about another person"; such hyperbole is unworthy of its authors.[9]

Rather than representing what one journalist dubs "a sinister law",[10] the privacy tort – just like the tort of defamation – is unlikely over time to result in substantial uncertainty for journalists and media proprietors and chill free speech.

Instead it can be readily reflected in professional codes of practice (albeit protocols of the Australian Press Council and journalism associations have been ineffective)[11] and should encourage public trust in the legitimacy of media organisations.[12]

Claim 4: the tort will prevent effective law enforcement and national security

As far as I am aware there have been *no* moves to establish a tort that comprehensively prevents lawful action by national security and the wide range of law enforcement agencies at the Commonwealth, state and territory levels. Claims that the tort will serve to shield the guilty, protect wrongdoers and inhibit legitimate policing are hyperbole. Those claims should be subject to rigorous analysis by the Commission.

---

[8] Chris Merritt, 'Legal Leader Denounces Gillard Government's Statutory Tort' *The Australian* (9 September 2011); and Robin Speed, 'No Need for Statutory Tort of Privacy in Australia' *The Australian* (4 November 2011).

[9] http://www.ruleoflaw.org.au/wp-content/uploads/2012/08/Media-1-9-11-Freedom-of-the-Press-and-Freedom-of-Speech-in-Australia-Robin-Speed.pdf

[10] Andrew Bolt 'Bad law, and worse motives' *Herald Sun* (10 September 2011)

[11] Note the critique in *Report of the Independent Inquiry into the Media and Media Regulation* (2012) (aka Finkelstein Inquiry). See also Bruce Baer Arnold, 'Self Regulation and a Media that we can trust?' *The Conversation* (17 April 2012) and 'Pressing On?: Privacy Frameworks and the Australian Media' (2012) 8(6) *Privacy Law Bulletin*.

[12] In that respect I note that much of the criticism of proposals for the tort have been associated with the News group. It is worrying that Mr Murdoch appears to have resiled from his acknowledgement in the House of Commons, following the Leveson Report, that News employees and associates systematically disregarded the privacy of a range of public and non-public figures. This submission is being made in a week that features the trial of one of the most senior executives of that group for egregious invasions of privacy. Litigation includes *Various Claimants v News Group Newspapers Ltd & Ors* [2013] EWHC 2119 (Ch); *Coulson v News Group Newspapers Ltd* [2012] EWCA Civ 1547; and *Bryant & Ors, R (on the application of) v The Commissioner of Police of the Metropolis* [2011] EWHC 1314 (Admin). News is reported to have spent over $100m in settlements and legal costs.

Australian law regarding privacy, from the colonial period onwards, has made considerable allowance for action by the state in undertaking law enforcement activity, in enabling intelligence gathering, in enabling information sharing to assist public administration and in facilitating counter-espionage activity.

Law has also permitted the disclosure of personal information by private/public actors in circumstances where that was necessary to prevent harm, along with scope for collection of information for the protection of interests. There is no reason to believe that the tort would override those statutes and judicial interpretation.

Instead, a potential criticism of proposals for the tort is that they are too weak rather than too strong.[13] One reason why establishment of the tort is desirable is that in the absence of a justiciable constitutionally-enshrined Bill of Rights its existence should encourage both regulatory coherence (ie rationalisation of the increasingly threadbare patchwork of privacy-related law across the Australian jurisdictions) and encourage community debate about privacy as a value that is integral to the respect for individual autonomy that underpins the liberal democratic state.

Privacy is not a middle-class fiction, with all respect to majoritarians such as Professor Bagaric, or a luxury that is necessarily sacrificed in dealing with terrorists or other threats. It is not antithetical to good government; pervasive surveillance by government agencies and their private proxies in the name of public safety instead reduces the trust in government that is fundamental to a vibrant civil society.

There is a place for surveillance by government. That surveillance must however take place on a lawful basis, something that should be regarded as different to what is bureaucratically convenient. The principles articulated in the ALRC paper mean that legitimate and proportionate action by law enforcement and national security agencies will not conflict with a statutory tort. In considering privacy beyond such a tort we should, I suggest, again be looking to principles and be wary about the administrative fixes inherent in 'legalising' activity that is not proportionate, effective and necessary.

Claim 5: the tort will flood the courts

The final claim is that a statutory or common law tort will result in frivolous or vexatious litigation, will flood the courts with inappropriate litigation and benefit legal practitioners rather than ordinary Australians. That claim can be examined from two perspectives.

The first is that Australia, along with the UK and similar jurisdictions, has enshrined the law of confidentiality (protecting commercial information and on occasion serving as a surrogate for privacy law) for more than 100 years. That law has *not* resulted in a flood of litigation. It has *not* unduly burdened the courts or served to foster vexatious and trivial action. Australia's experience with the law of confidence demonstrates that the harms forecast by critics of the statutory privacy tort are without foundation. Confidentiality has *not* shielded wrongdoers, has *not*

[13] The proposals do not for example address large scale data collection by the Australian Signals Directorate under the *Intelligence Services Act 2001* (Cth) and the exchange of information with other governments or more specific collection by ASIO under the *Telecommunications (Interception and Access) Act 1979* (Cth), ie activity that *is* lawful but for example has recently attracted adverse comment after revelations about the US PRISM initiative.

fundamentally weakened national security or legitimate policing (ie policing that is authorised by law rather than what is merely convenient) or crippled free speech. It has indeed been used by journalists, media proprietors and officials to strengthen their positions. Its existence provides a benchmark for testing hyperbole about the tort.

As a corollary, we should accord all Australians the respect due to them and not deny their access to law. If people – as individuals or on a representative basis – wish to take action in response to a serious invasion of privacy they should indeed be permitted to do so.[14] They should not have to rely on a handful of Commonwealth officials to act in their interest, a reliance that is problematical because of the bureaucratic incapacity acknowledged by the OAIC. They should also not have to rely on public shaming, by for example an MP or the mass media or an industry ombudsman, to secure an apology or compensation of that invasion or deterrence of a future invasion.

Australian courts have over many years shown the ability to provide measured judgments in response to a range of torts. There is no reason to believe that introduction of a statutory tort will result in an unprecedented 'rush of blood to the head' or ongoing confusion. A cautious approach by the superior courts in interpretation of the statute and adherence to the doctrine of precedent means that within a decade or so we are likely to be asking what all the fuss was about, in the same way that doomsaying at the time of introduction of the *Privacy Act 1988* (Cth) and *Freedom of Information Act 1982* (Cth) has not been substantiated.

As a point of reference I note that recognition of a common law tort in New Zealand has *not* flooded that nation's courts, has not resulted in the death of the NZ media industry, has not chilled free speech. The tort has not inhibited law enforcement action or national security legislation such as this month's *Telecommunications (Interception Capability and Security) Act 2013* which gives considerable leeway regarding law enforcement.[15] There is no reason to believe that introduction of a statutory tort in Australia would have a different result.

Hyperbole by critics of a tort should be recognised by the Commission as uninformed or special pleading by vested interests, rather than claims that are persuasive.

Approach

Australian law regarding privacy has been bedevilled by regulatory incoherence. That incoherence reflects inconsistency across the various jurisdictions. Given Australia's

[14] It is puzzling that entities advocating 'the rule of law' are disquieted by the prospect of litigation that addresses activity that is outside the law or should be considered outside the law. The ability to address harms should not be restricted to corporations and individuals with deep pockets. We should be wary of reinforcing the aphorism that freedom of the press belongs to those who both own a press and can afford the associated silks. The principle of 'access to justice' highlighted by the Commission is important.

[15] For New Zealand see *Hosking v Runting* (2004) 7 HRNZ 301; [2005] 1 NZLR 1. It is notable that there is no indication that New Zealand journalists have become more cautious in exposing wrongdoing. See also *P v D* [2000] 2 NZLR 591 and the discussion in New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies (Review of the Law of Privacy)* (NZLC Report No 113, 2010) 91. Comparable jurisdictions have provided statutory coverage, with Saskatchewan for example giving a statutory recognition to 'a tort, actionable without proof of damage, for a person willfully and without claim of right, to violate the privacy of another person'. The Ontario decision in *Jones v Tsige* [2012] ONCA 32 (CA) is considered in Bruce Baer Arnold 'Coming here? The Canadian privacy tort: Jones v Tsige [2012] ONCA 32 (CA)' (2012) 8(5) *Privacy Law Bulletin* 80.

commitment to both international human rights agreements and integration with the global economy it is worrying that the recognition of privacy varies from one state to another.

Incoherence also reflects the haphazard accretion of statute and common law, which has typically been technology-, use- and agency- specific (eg covering audio listening devices but not audio-video devices, networked but not standalone surveillance tools, action by public but not private investigators, information privacy but not other privacy, government agencies but not small businesses, educational institutions but not political organisations).

It has provided weak remedies for individuals who have experienced a serious invasion of privacy, for example are unlikely to gain compensation through a victims of crime regime in relation to an offence under crimes statutes and may have difficulty relying on a breach of confidence for damages.

A statutory cause of action, with a range of remedies, is important in both addressing specific invasions of privacy and more broadly in articulating principles that are founded on the respect for dignity that has been highlighted above. In essence, the Australian legal system both can and should recognise privacy as foundational and as broader than the information privacy that is inadequately addressed through the amended *Privacy Act 1988* (Cth).[16]

The ALRC paper is especially valuable because of its emphasis on principles. Those principles should be specifically articulated in Commission's report, featured in the statute and glossed in extrinsic interpretation aids such as the explanatory memorandum. As such they will serve two key functions.

Firstly, they will signal that privacy is not a fiction or a luxury but is instead integral to the flourishing of Australians as members of a liberal democratic state, ie as autonomous individuals who have both rights and responsibilities in their personal and social lives. It is a basis for flourishing rather than antithetical to commerce and good government. Irrespective of remedies for specific harms to individuals, establishment of the tort will go some way to addressing perceptions in the community that people are doomed to disregard of their privacy and therefore should not bother with self-management.

Secondly, the principles will address the hyperbole – in some instances disinformation – from vested interests that the tort will result in harms such as excessive, frivolous or vexatious litigation or that it is inconsistent with media freedom and law enforcement.

This submission accordingly endorses the principles identified by the ALRC, ie

- 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

[16] The reference to inadequacy reflects both the technical incapacity of the Office of the Australian Information Commissioner, which lacks resources and has been very reluctant to use its moral authority to offset that weakness. It also reflects the weakness in the legislation, which does not cover small business and that is reliant on codes that in practice are developed by industry and only notionally supervised by the OAIC.

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

Bruce Baer Arnold
Assistant Professor, Law
University of Canberra

11 November 2013

Response to specific questions

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 principles identified in the ALRC paper are endorsed. They should be regarded as an aggregate, ie not 'cherry-picked' or weakened through exclusions on the basis of sector or technology.

They should be implemented on a holistic basis and it is thus appropriate to conceptualise a single tort rather than differentiation, for example, between an information privacy tort and a separate spatial or other non-data tort. As indicated in the separate Australian Privacy Foundation submission, privileging one attribute (for example bureaucratic convenience in the enforcement of civil or criminal law) over principles results in law and practice that lacks legitimacy and coherence.

In particular the ALRC should explicitly and strongly resist suggestions to 'stack' rights in a hierarchy that privileges the interests of broadcasters, connectivity providers and social network services or law enforcement personnel.

Australian jurisprudence regarding confidentiality, defamation and national security has demonstrated that courts are fully capable of identifying public interest and of dealing with tensions in claims regarding public good.

Those courts are capable of discerning what is legitimate and proportionate, what is trivial, and what are appropriate remedies.

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.

In responding it may be useful to note that the Commission is concerned with serious invasions of privacy, ie excludes activity that is trivial or frivolous. The Commission's examination implicitly excludes law enforcement and national security activity, presumably on the basis that such activity will be necessary, legitimate and proportionate.

The law reform commission/committee reports noted above identify invasive activities that are inadequately addressed under Commonwealth and state/territory statute and common law. In considering responses to the current paper I suggest that the Commission place less emphasis on specific activities or technologies (such as cheap drones, lapel cameras and pen recorders) and more emphasis on principle.

The salient concern should be on 'serious invasion', which can be addressed on a flexible basis by Australian courts and does not require a detailed taxonomy or borrowing of the categorisation articulated by for example Prosser in the United States.[17] An over-emphasis on types of technologies and specific actions runs the risk

[17] Prosser is of only marginal relevance, given that US conceptualisation about harms, rights, responsibilities and remedies is embedded within a very different jurisprudence and body of statute law founded on the Bill of Rights. That conceptualisation has increasingly sacrificed private life to the

of perpetuating the existing technology and jurisdiction silos that result in injustice and confusion.

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?

As above, there is value in referring during the Commission's final report (and in any extrinsic material for statutory interpretation) to examples of activity that is inappropriate on the basis of the principles. The risk in any tabulation of restricted and unrestricted activities is that the listing will be read in a way that is contrary to the principles and thus serves to erode the objects of the statute. An emphasis on principle should encourage courts in interpreting the statute to look beyond specific circumstances and encourage entities that are experiencing or engaging in serious invasions to understand what the tort the tort is meant to do.

In making that comment I stress, as in the Australian Privacy Foundation submission, that the tort is not antithetical to law enforcement, national security or appropriate private self-help (eg recording by a person who is being threatened). Law enforcement or other activity that is however *not* appropriate and proportionate should however be restricted; 'legalising' abhorrent activity through statute should raise concerns among policymakers, legislators and ordinary people but on occasion will not be readily discernable because of weaknesses in the Australian access to information regime (eg imposition of inappropriate costs and comprehensive redactions in response to Freedom of Information applications).

In considering what is 'unduly' restrictive it is important to acknowledge substantial weaknesses within the *Privacy Act 1988* (Cth) and other legislation that feature substantial formal 'carve-outs'. Those carve-outs are exacerbated by regulatory incapacity (lack of power, expertise and initiative) on the part of the Office of the Australian Information Commissioner and other entities such as the Australian Communications & Media Authority. It is highly undesirable that the scope for action regarding serious invasions of privacy be seriously eroded through major exemptions, through reference to a regulator that is inactive or reliance on permissive industry codes such as those used by the Press Council. People who have experienced a serious invasion of privacy should have scope to make a complaint to the relevant regulator. They should not however be forced to go to that regulator and any approach to the regulator should not preclude private action under the tort.

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?

Examples rather than a restrictive listing would be useful in guiding courts, marketers, journalists, officials and consumers. Inclusion of examples would also be of value in anticipating unfounded anxieties about the purpose of the legislation or its scope.[18] Inclusion of examples in the statute rather than merely in extrinsic aids to interpretation is not remarkable or inconsistent with Australian drafting practice.

The list should be clearly identified as non-exclusive, ie should be regarded as

---

desire for 'news', privacy to a 'right to sensation'. If we are benchmarking we should as a society be also referring to the growing and judicially persuasive body of data protection law and human rights law in the European Union.

[18] Your attention is for example drawn to description by one individual of the proposed statute as a "sinister law" by a government with "sinister motives", a characterisation that has regrettably been embraced by some advocates within the legal profession.

illustrative rather than exhaustive. Courts should be able to deal with serious invasions of privacy that fall outside the list, consistent with 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?

Given the emphasis on principle there is no value in differentiation between two or more causes. The emphasis should be on serious invasion and the statute should not be expressed in a way that leads either courts or the entities that engage in invasion to construe seclusion as necessarily more/less serious than private information.

That comment is consistent with the potential for the *Privacy Act 1988* (Cth) and any associated data breach statute to offer a 'lite' remedy for invasion of private information, particularly if there is an expectation in law that

- private information problems will be addressed by a handful of officials (in the first instance the OAIC) and
- intrusion on seclusion will be addressed by a mix of a Commonwealth tort and state/territory criminal law.

The emphasis should be on privacy and serious invasion *per se*, rather than particular demarcations.

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?

The terms of reference for the Commission's inquiry refer to serious invasion, something that precludes private action over what is trivial or frivolous.

A 'reasonable expectation of privacy' is flexible and consistent with the principles noted above. One criticism may be that 'reasonable' is too vague or fluid and thus encourages uncertainty. A direct response is that both Australian and UK courts over the past century have been able to deal with notions of what is reasonable (for example in relation to confidentiality). The test can be interpreted by the courts to reflect principles and evolving social practice.

Consistent with the separate APF submission, serious invasion should not be predicated on psychiatric or other harm to the individual whose privacy has been invaded. The tort should in the first instance be addressing the *invasion* – the disregard of privacy, of dignity, of human rights – rather than any harm.[19] It is important in signalling and deterring wrongdoing rather than merely providing compensation for an injury.

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?

Perceived and substantive conflicts of public interest, reflected in the principles, can

[19] The severity of different harms can be addressed in an instance by instance basis through the remedies discussed below.

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 priorities law enforcement or the implied freedom of political communication or the commercial media over respect for the individual whose privacy has been invaded.

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.[20] 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.

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

Given the above, it is not necessary for the Act to provide detailed guidance about the nature of public interest or about a stacking of public interests that serves to erode what should be regarded as the raison d'etre of the statute. The onus of persuading the court that there is a compelling public interest that justified a serious invasion of privacy should rest with the defendant. As above, I note the importance of differentiating between public curiosity (and the revenue gained by media organisations in satisfying that curiosity) and public interest, in particular the public interest in recognising and encouraging the autonomy and dignity of members of society in a liberal democratic state. Detailed guidance may indeed have an unintended and undesirable outcome by being read exclusively.

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?

As per above the cause of action should encompass serious invasions of privacy *per se* and should accordingly include negligence.[21]

The past decade has seen a succession of revelations of privacy breaches attributable to indifference and incapacity on the part of health service providers, educational institutions, financial institutions, government agencies, connectivity providers and other entities. That behaviour has on occasion been tacitly accepted by the Office of the Information Commissioner as inevitable, an acceptance that normalises invasions or information management weaknesses that facilitate serious invasions. Action for negligence provides a necessary and appropriate incentive for Australian organisations to move towards best practice in information management. An emphasis on what is proportionate and legitimate should suffice to address anxieties that individuals and organisations will be inappropriately exposed to private litigation on the basis of negligence

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

---

[20] See for example *Commonwealth v John Fairfax* (1980) 147 CLR 39; *Commonwealth v John Fairfax* (1980) 147 CLR 39 *G v Day* [1982] 1 NSWLR 24; *Attorney General (UK) v Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30; *Westpac Banking v John Fairfax Group* (1991) 19 IPR 513

[21] That scope excludes trivial invasions, which accordingly do not need to be addressed in terms of negligence.

The cause should be actionable *per se*.

That comment 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.

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)?

In the preceding comments I have suggested that the cause of action should be concerned with serious invasion. It should not be restricted to psychiatric injury or narrowly construed in terms of ongoing embarrassment or ongoing/short term emotional distress.

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. Reference to what is proportionate, necessary, reasonable and lawful is an essential requirement.

In preceding comments I have noted the concern within the legal community and wider community about 'legalising' activity by the state that is bureaucratically inconvenient but contrary to trust in government and contrary to human flourishing. We have seen a succession of national, state and territory governments pass legislation that impinges on civil liberties and that on occasion has been rejected by the High Court. The absence of a constitutional enshrined (and thus justiciable) Bill of Rights means that governments will continue to enact law that poses substantive and legitimate concerns regarding civil liberties. The Commission in its final report may wish to highlight those concerns while conceding that a tort will only be accepted by a national government if the statute provides a substantial carve-out for the activity of a range of agencies. Overall the emphasis of that carve-out should be on what is reasonable, necessary and proportionate rather than what is merely legal. Australian courts are equipped to determine what is proportionate, necessary and reasonable. European jurisprudence on matters such as mandatory data retention provides some guidance about those questions, more so than reliance on US law.

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?

Public interest, as per above, is more useful than defamation-based defences such as qualified privilege. There is disagreement within the legal and information technology communities regarding the potential liability of intermediaries for serious infringement, including questions about whether search engines and social network services will be able to evade responsibility if the law features a defamation-style defence of innocent dissemination and use is made of a weak prescribed take-down protocol that is not readily accessible by individuals whose privacy has been seriously infringed (given for example consumer criticism of difficulty in triggering such takedowns and delays in action by social network service operators). The matter

might be covered by the ALRC in the next paper.

Work by Australian academic David Lindsay on the 'right to be forgotten' is particularly relevant.

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

Addressing the tort on a holistic basis and emphasising public interest, as per above, obviates the need to provide a tight statutory taxonomy of circumstances in which privacy breaches may be justified. A close categorisation of defences poses a substantial risk that some serious invasions will be excluded from coverage because of the inadequacy of drafting.

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

Given the above comments there is no need for a categorisation of exclusions.

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?

Consistent with the above comments the enactment should cover damages, an account of profit, apology, retraction and injunction.

The Act should not restrict remedies by setting a ceiling, ie specifying a maximum award of damages. Such a restriction reduces flexibility and is unnecessary, given that Australian courts have demonstrated a common sense approach in the provision of remedies.

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)?

The statement of principles should provide guidance for courts. Australian courts, following the High Court, have not enshrined a broad freedom of expression; expression is instead construed in terms of public benefit rather than as a 'super-right' that trumps all law or that for example privileges public curiosity (under the rubric of 'news') over the privacy of celebrities and non-celebrities alike.

There is some value in incorporating a provision such as s 12 of the *Human Rights Act 1998* (UK) rather than merely an explicit reference to 'freedom of political communication' but the expectation should be that courts would consider that freedom in terms of public interest. EU jurisprudence on public interest in relation to privacy is instructive.

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 should be included as a non-monetary remedy, given that some subjects of

serious invasion may not be interested in financial compensation and may for example be primarily concerned to

- deter future invasions of the privacy of peers who are less resilient
- gain a private statement of contrition
- publicly vindicate claims that their privacy was indeed invaded on a basis that was neither lawful nor reasonable
- gain community recognition through a public apology that the invasion is abhorrent and actionable (as distinct from deeply distressing but without a remedy).

Privacy as a human right should be restricted to natural persons. There are existing and adequate remedies for public/private organisations that experienced unauthorised access to and/or threatened/actual misuse of personal information. In particular Australian law provides for confidentiality in relation to corporations and action under the tort should not be brought by a corporate person in its own right.

Serious invasions should be actionable by a minor's parent or by a guardian on behalf of a subject, a matter that is gaining increasing judicial interest in Europe. Parents for example may well have become hardened to invasions of their privacy as celebrities (and often in a better position to evade invasions) but legitimately be concerned to protect the privacy of their children and therefore wish to take action.

The tort should be actionable on a representative basis, given multiple people may be the subject of a serious invasion by an organisation. Representative action offsets differentials in power and is consistent with the principle regarding access to justice. Emphasis on serious invasion should offset concerns that representative action will result in inappropriate litigation that clogs the courts, inappropriately rewards legal practitioners and deals with trivial invasions.

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 emphasis on principle and on one role of the tort in signalling the tort should survive the deceased person and not be limited to pecuniary losses or dependent on emotional distress. It should thus be regarded as different to defamation action.

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?

As has been recurrently highlighted by privacy specialists and public policy analysts, the various privacy/information commissions are problematical because of weak charters (centred on information privacy), exposure to ongoing budget cuts and in some instances a reluctance to use soft power – moral authority in the absence of black letter power – in reproving privacy abuses by public/private sector entities such as Australia's largest telecommunication service providers.[22] A key rationale for recognition of the tort is that it will allow people who have experienced a serious

[22] Ongoing FOI-based research at the University of Canberra appears to suggest that the OAIC is in fact not being consulted in detail about privacy law development, is in an adverse position in competition with better-resourced (or more vigorous) agencies such as ACMA, and in practice is being disregarded by entities such as the Australian Federal Police.

invasion of privacy to take action independently of the OAIC or other government agency, something that is likely to provide victims with what they see as an acceptable outcome and may encourage those agencies to be more vigorous.

Those people should not be precluded from making a complaint to the OAIC (or its state counterparts). The OAIC may legitimately conduct an inquiry in response to such a complaint or on an own motion basis, reflecting the new Australian Privacy Principles. It should not however have sole responsibility for action.[23] Given the likelihood that the OAIC will continue to experience resource problems there should be no requirement that people initially seek a resolution via the OAIC or that the availability of action is subject to failure of a conciliation exercise under the OAIC.

Similarly there should be no requirement that people must initially seek a remedy through the Press Council or another industry body. The weakness of the Press Council remains of fundamental concern, exacerbated by statements that some media groups will withdraw to wholly self-regulate. Industry bodies can and should provide guidance to both their members and the wider community about privacy practice, a guidance that may well be useful for courts in determining what is reasonable, proportionate, negligent and so forth.

An emphasis on litigation by the subjects of a serious invasion (rather than conciliation by the OAIC or by a nongovernment body such as the Press Council) is not ideal, given that some victims may lack the funds or understasnding to exercise their rights. It is however consistent with other areas of law (for example confidentiality) and is a practical solution. It should be for the courts and the national legislature to consider what is a serious invasion and provide an appropriate remedy. Responsibility should not be left to a handful of Commonwealth officials.

An issue underlying questions about the tort is where we place the statutory provisions. At the moment there are over 300 statutes that are devoted to privacy or data protection or that features privacy provisions. As noted above the *Privacy Act 1988* (Cth) is concerned with information privacy. It sits alongside other Commonwealth privacy statutes. Inclusion in the 1988 Act will reshape that statute. There has however been no indication from the Commonwealth government that it is concerned to achieve a more coherent national privacy regime through a comprehensive revision of the Act.

Inclusion of the tort within the Act threatens to weaken the tort, through for example linking it closely to the OAIC in ways that would inhibit private action.

I accordingly suggest that, pending a 'root & branch' revision of the 1988 Act, the tort be dealt with through discrete legislation. A precedent for a discrete enactment is provided by the defamation statutes in most jurisdictions.

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?

The limitation should start from when the subject becomes aware of the invasion, an awareness that in some instances may be instantaneous and in others may not arise until a considerable time after the invasion has commenced or concluded. There is

[23] In that respect it is useful to note that in the broadcasting and telecommunications sector ACMA and the OAIC have been conducting overlapping investigations into privacy abusers and data breaches, with ACMA typically reporting in more detail several months ahead of the OAIC and appearing to offer sterner warnings (attributable to corporate style rather than merely statutory power) than the OAIC.

no ideal period for the conclusion of the limitation period, although the defamation model (ie one year) appears viable.

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?

As noted above, cause should be located in discrete legislation rather than within the *Privacy Act 1988* (Cth), reflecting both the need to provide consistent national coverage of activity in the various jurisdictions and the current statute's emphasis on information privacy.

Privacy as a human right is properly regarded as a national responsibility and for a coherent nationwide regime the cause should be located in Commonwealth statute law, which encourages ready identification and understanding by specialists and non-specialists alike. The constitutional basis for that legislation is provided by the external affairs power (reflecting Australia's participation in human rights agreements, recognised by the High Court). That power is more viable than reliance on sectoral powers regarding telecommunications and corporations.

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

The availability of action does not preclude public/private conciliation mechanisms and on occasion some invasions may be addressed to the satisfaction of all parties through a confidential apology that does not involve any mediation.

In terms of action, as a matter of national interest under a national statute and national constitutional head of power the Federal and Supreme Courts are appropriate fora.

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

In preceding comments I have noted that some invasions may result in an investigation (and even imposition of a penalty) by the OAIC on an own motion basis or in response to a complaint. Some parties may wish to use alternative dispute resolution mechanisms (including bodies under industry auspices) on the basis of privacy, speed of resolution, cost and minimisation of stress and given this submission's emphasis on autonomy should be allowed to use those mechanisms. However, there should be no mandating of those mechanisms and consumers should not be held to waive rights to take action by agreeing to a 'click-wrap' agreement on a social network service or other site that purports to void statutory protections. Work by the Article 29 Working Party on consent in online activity is particularly relevant. There should be no requirement for initial conciliation by the OAIC, given substantive concerns regarding that agency's regulatory capacity, and no exclusion from action if conciliation or investigation by the OAIC was unsatisfactory. In practice the scope for action outside the *Privacy Act 1988* (Cth) and the OAIC should serve to keep the latter 'on its toes' rather than marginalising the agency or weakening the 1988 statute.

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?

Statutory recognition of the tort outside the *Privacy Act 1988* (Cth) will serve to reinforce awareness that a determination under the 1988 Act does not preclude a claim based on the statutory cause of action. There is no reason to believe that scope for such a claim will result in vexatious litigation that cannot be effectively addressed by the courts or that it will result in major uncertainties or administrative inefficiencies across the justice system.

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?

As noted above the tort has been recommended by Commonwealth, NSW and Victorian law reform bodies over several years. It has a sound basis and should be adopted.

The state, territory and national legislatures should be encouraged to strengthen privacy protection generally. Preceding comments noted inconsistencies in state/territory law regarding surveillance devices. Those inconsistencies could be addressed in a way that complements the establishment of a national cause of action rather than ostensibly removes the need for a national statute.

The preceding comments have also highlighted concerns regarding 'legalisation' of activity by law enforcement and national security bodies that is invasive and that some Australians would consider to be commercially onerous (eg mandatory data retention) or consider to be unreasonable or disproportionate. Rather than relying on piecemeal statutory change as a *substitute* for establishment of a national tort, we should as a society be engaging in a debate about privacy rights, responsibilities and mechanisms as the basis for a coherent and progressive regime.

In advising the Attorney-General the ALRC has an opportunity to foster the informed development of policy by highlighting the need to

- explore what has been characterised as 'the right to be forgotten'
- revisit reports on the liability of intermediaries in the digital environment
- reflect data protection and privacy law development within the European Union, ie a major trading partner
- achieve greater transparency in the development and adoption of frameworks such as the TransPacific Partnership Agreement[24]
- achieve consistency in surveillance devices law, including activity in the private and public sectors, and to fix gaps in privacy protection attributable to sectoral demarcations
- address concerns about law enforcement developments relating to events such as the G20 meeting and to subjects of moral panic such as outlaw motorcycle gangs

[24] Details of the TPPA remain secret and it is clear from the very limited public consultations that have taken place that many officials with an interest in privacy, rather than people outside government, are unaware of what is contemplated. There have been indications that the TPPA will have a substantial impact on privacy law and practice; lack of transparency is thus of great concern.

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?

As per **Q26**.

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

As per **Q26**.