



11 November 2013

Professor Barbara McDonald
Commissioner
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

By email to: info@alrc.gov.au

Dear Ms McDonald

Inquiry into Serious Invasions of Privacy in the Digital Era

The Law Institute of Victoria welcomes the opportunity to provide comment on the Issues Paper, Serious Invasions of Privacy in the Digital Era (ALRC Issues Paper 43, 2013). Our submission is attached.

Please contact Courtney Guilliat, Policy Adviser for the Administrative Law and Human Rights Section, on (03) 9607 9375 or cguilliatt@liv.asn.au in relation to this submission.

Yours sincerely,

Reynah Tang
President
Law Institute of Victoria

The Law Institute of Victoria
is a member of



Law Council
OF AUSTRALIA

Law Institute of Victoria Ltd

ABN 32 075 475 731

Ph (03) 9607 9311 Fax (03) 9602 5270

Email lawinst@liv.asn.au

470 Bourke Street Melbourne 3000 Australia

DX 350 Melbourne GPO Box 263C Melbourne 3001

Website www.liv.asn.au



Serious Invasions of Privacy in the Digital Era

To: Australian Law Reform Commission

11 November 2013

Queries regarding this submission should be directed to:

Contact person Courtney Guilliat
Ph (03) 9607 9375
Email cguiliatt@liv.asn.au

Table of Contents

Introduction	4
Principles guiding reform	4
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?	4
The impact of a statutory cause of action	5
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.	5
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?	6
Invasion of privacy	7
Question 5. What, if any, benefit would there be in enacting separate causes of action for: misuse of private information; and intrusion upon seclusion?	7
Privacy and the threshold of seriousness	7
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?	7
Question 7. How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:	8
• competing public interests must be considered when determining whether there has been a serious invasion of privacy; or	8
• public interest is a defence to the statutory cause of action?	8
Question 8. What guidance, if any, should the Act provide on the meaning of ‘public interest’?	8
Fault.....	9
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?	9
Damage	10
Question 10. Should a statutory cause of action for serious invasion of privacy require proof of damage or be actionable <i>per se</i> ?	10
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)?	10
Defences and exemptions	11
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?	11
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?	11
Question 14. What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?	11
Question 15. What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?	12

Monetary remedies	12
Question 16. Should the Act provide for any or all of the following for a serious invasion of privacy:.....	12
• a maximum award of damages;.....	12
• a maximum award of damages for non-economic loss;.....	12
• exemplary damages;.....	12
• assessment of damages based on a calculation of a notional licence fee;.....	12
• an account of profits?	12
Injunctions	13
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)?	13
Other remedies	13
Question 18. Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action?	13
Who may bring a cause of action	13
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?.....	13
Limitation period	14
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?	14
Location and forum	15
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?.....	15
Question 23. Which forums would be appropriate to hear a statutory cause of action for serious invasion of privacy?.....	15
Question 24. What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?.....	15
Interaction with existing complaints processes	16
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?	16
Other legal remedies to prevent and redress serious invasions of privacy	16
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:	16
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?	17
Question 28. In what other innovative ways may the law prevent serious invasions of privacy in the digital era?.....	17
Further contact	18

Introduction

The Law Institute of Victoria (LIV) welcomes the opportunity to comment on the Australian Law Reform Commission (the Commission) Issues Paper, *Serious Invasions of Privacy in the Digital Era*. The right to privacy, and the need to balance that right with other rights, is an important issue for the LIV. The LIV has been a long-standing supporter of a statutory cause of action for invasions of privacy. Submissions made by the LIV on privacy related issues include:¹

- Inquiry into the *Privacy Act 1988* (Cth) (25 February 2005)
- Australian Law Reform Commission *Issues Paper: Review of Privacy* (21 February 2007)
- Victorian Law Reform Commission *Consultation Paper: Surveillance in Public Places* (6 July 2009)
- Senate Standing Committee on Environment, Communications and the Arts inquiry into the adequacy of protections for the privacy of Australians online (29 July 2010) and supplementary submission (20 December 2010)
- Exposure Draft of the Australian Privacy Principles (19 August 2010)
- Inquiry into Exposure Drafts of the Australian Privacy Amendment Legislation - Credit Reporting (31 March 2011)
- Department of Prime Minister and Cabinet *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (18 November 2011)
- Inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) (9 July 2012)
- Letter to the Victorian Attorney-General on privacy protection in Victoria (8 November 2012)

The LIV also called for a statutory cause of action for invasions of privacy in our policy on privacy adopted in November 2011.²

The LIV submission on the Issues Paper draws heavily on the submission it made to the Department of Prime Minister and Cabinet on 18 November 2011 and responds to select questions and key issues raised in consultation with the Commission on 17 October 2013.

Principles guiding reform

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 LIV welcomes the Commission's inquiry into a statutory cause of action for serious invasions of privacy. The LIV supports the creation of a statutory cause of action by way of a Commonwealth Act, which is flexible, accessible and appropriately contained.

Rapid advances in information, communication, storage, surveillance and other relevant technologies have significant implications for individual privacy. The 2013 Office of the Australian Information Commissioner Community Attitudes to Privacy survey reported that Australians believe the biggest privacy risks facing the community are online services, including social media sites.³ The ability of people to protect and control their personal information is clearly a growing concern in the digital era.

¹ All submissions are available on the LIV website: <http://www.liv.asn.au/For-Lawyers/Sections-Groups-Associations/Practice-Sections/Submissions>.

² LIV, *Policy on privacy-related issues in laws and government policy* (November 2011) <<http://www.liv.asn.au/About-LIV/LIV-Management---Governance/LIV-Policy-Statements>>.

³ Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey Research Report* (2013), p3 <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013>>.

In its 2011-2012 Annual Report, the Office of the Australian Information Commissioner reported that there were 1357 privacy complaints, 126 freedom of information complaints, 456 applications for Information Commissioner review and the office conducted 37 privacy own motion investigations.⁴ In its 2012 – 2013 Annual Report, the Office of the Victorian Privacy Commissioner reported that with the exception of two reporting periods new complaints have risen gradually over the past ten reporting periods, levelling out in 2012-13.⁵ Consistent with the rise in privacy complaints, we note that the right to privacy is consistently found to be the most frequently invoked right in cases in which the *Charter of Human Rights and Responsibilities Act 2006* (Vic) has been raised since it entered into force in 2007.⁶

In Victoria, the right to privacy is protected under the *Charter of Human Rights and Responsibilities Act 2006* (Vic). Several Victorian laws protect information privacy, such as the *Victorian Information Privacy Act 2000* and the *Health Records Act 2001*. Some common laws might be engaged where particular actions affect a person's privacy.⁷ At a Commonwealth level, privacy is regulated by the *Privacy Act 1988* (Privacy Act). Many changes to the Privacy Act introduced by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* will commence in March 2014. These changes are part of a wider law reform process that extends back to the Commission's inquiry into privacy law and practice in 2006. The right to privacy is also protected at an international level under the International Covenant on Civil and Political Rights.⁸

The LIV agrees with the Commission that there is a need for a cause of action for serious invasions of privacy in Australia. As the LIV has previously argued, existing laws and codes of conduct are piecemeal and inadequate in scope and force, offering limited remedies and leading to insufficient incentives for compliance or pursuing complaints. The common law evolves to accommodate individual cases and it takes too long to develop elements of general application, during which time uncertainty as to the nature and scope of the law prevails. Relying on piecemeal protection increases the costs and complexity of taking action in relation to privacy breaches.

The LIV considers that the Commission's approach to the inquiry should be guided by the following principles:

- Persons have a right not to have their privacy unlawfully or arbitrarily interfered with. The LIV believes that the protection of an individual's privacy is fundamental to their human dignity and is central to many other human rights such as the right of freedom of association, movement and expression;
- The right to privacy should be balanced with other rights in the public interest, such as the right to freedom of expression and participation in public affairs;
- Any cause of action for serious invasions of privacy must be accessible to all people who are subject to invasions of privacy.

The impact of a statutory cause of action

Question 2. What specific types of activities should a statutory cause of action for serious invasion of privacy prevent or redress? The ALRC is

⁴ Office of the Australian Information Commissioner, *Annual Report 2011 – 2012* (28 September 2012), p4 <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2011-12/OAIC_annual_report_2011-12.pdf>.

⁵ Office of the Victorian Privacy Commissioner, *Annual Report 2012 – 2013* (September 2013) p10, <[https://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/annual-report-2012-2013/\\$file/annual_report_12_13.pdf](https://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/annual-report-2012-2013/$file/annual_report_12_13.pdf)>.

⁶ LIV, *Charter Case Audit* (December 2012) <<http://www.liv.asn.au/PDF/For-Lawyers/Submissions-and-LIV-Projects/LIVCharterCaseAudit2013>>.

⁷ Compensation was awarded for 'hurt, distress, embarrassment, humiliation, shame and guilt' in respect of breach of confidence in *Doe v ABC & Ors* [2007] VCC 281, para 186, a case concerning media disclosure of the identity of a rape victim. See further *Doe v ABC – A new version of a privacy tort?* Graham Greenleaf, 23 April 2007, AustLI.

⁸ Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

particularly interested in examples of activities that the law may not already adequately prevent or redress.

The LIV does not consider that any statutory cause of action should be designed in order to prevent a particular type of invasion of privacy. Any statutory cause of action should be sufficiently flexible and adaptable to address a range of serious invasions of privacy, which will depend on the facts and circumstances of the particular matter.

However, we also consider that a statutory cause of action has the potential to address the significant gaps in current privacy protection in Australia. These gaps are, in part, attributable to the rapid advances in technology, especially since 2006, when the Commonwealth Attorney-General referred to the Commission for inquiry matters relating to the extent to which the Privacy Act continued to provide an effective framework for protection of privacy in Australia.

Current laws have been ineffective in addressing a range of privacy concerns, including:

- the increased, but arguably unnecessary, collection of data by companies, including scanning and retention of personal identification at venues including pubs and clubs;
- compulsory collection of personal information about individuals (used for advertising purposes) in order to obtain goods or services;
- activities of small businesses and political parties which are exempt from the operation of the Privacy Act; and
- the impact of social media in areas of the law including litigation, family law, workplace relations and defamation cases. We note in particular the use of social media platforms by parties to family law proceedings to post invasive photos or information.⁹

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?

The LIV does not support exclusions for specific organisations, types of organisations or activities. Privacy is contextual and depends on facts and circumstances. Attempts to exclude small businesses, political parties and media organisations (all of which are exempt to some extent from the Privacy Act) would entrench the current gaps in privacy protection in Australia, which lead to limited or no legal redress for people who experience serious privacy invasions in certain contexts. Continuing these exemptions would undermine the effectiveness of any cause of action.

The LIV recommends that careful consideration be given to how the cause of action would relate to individuals responsible for serious privacy invasions. Currently, individuals are included in the definition of 'organisation' under the Privacy Act and, therefore, prima facie, the National Privacy Principles apply against individuals for invasions of privacy. However, we are not aware of any matters in which action has been taken against individuals under the Privacy Act and it is by no means certain that the application of the National Privacy Principles against individuals, without amendment, is appropriate. We note that this is not an issue that has been considered at length.

While individuals should not necessarily be excluded from the ambit of a cause of action for serious invasions of privacy, the Commission should consider carefully how the responsibilities of business and government under a cause of action would translate to individuals. It should not be assumed that the statutory cause of action would have the same effect on individual defendants as corporate or government defendants.

⁹ See, for example, the cases cited by The Honourable Justice Garry Watts, 'Social Media and Family Law' (Speech delivered at the Australian Family Law Conference, Singapore, 10 – 14 June 2011).

Invasion of privacy

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?

The LIV has previously argued that it would not be appropriate to include in any legislation establishing a cause of action for privacy invasions a non-exhaustive list of activities that could constitute an invasion of privacy. The LIV would hold the same concerns with a list of examples of invasions of privacy. As previously stated, the LIV feels this would be of limited assistance to a court and might give would-be defendants the impression that conduct outside the parameters of the list does not constitute an invasion of privacy. In the current technological age, it is likely that any examples in a list could be quickly superseded by other types of privacy invasions that might evolve in the future. Furthermore, privacy is contextual and depends on facts and circumstances. For these reasons, a list of examples will rarely be helpful.

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 LIV would not support separate causes of action for misuse of private information and intrusion upon seclusion. A statutory cause of action should address both information and spatial privacy, where information privacy refers to 'control over access to private information or facts about ourselves' and spatial privacy refers to 'control over access to our persons and to private spaces'. Specificity is needed to describe the parameters to any cause of action, however, two causes of action could cause confusion and might exclude other appropriate grounds for an action.

The LIV has previously argued that a better option is to provide a single cause of action and include in the definition of 'privacy' the concepts of information privacy and spatial privacy.

Privacy and the threshold of seriousness

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 LIV submits that a cause of action for privacy invasions should be based on there being 'a reasonable expectation of privacy' and limited to 'serious' invasions. In its submission to the Department of Premier and Cabinet in 2011, the LIV did not support the inclusion of an additional requirement that the invasion be 'highly offensive' to a person of ordinary sensibilities.

First limb: 'Reasonable expectation of privacy'

The LIV considers that a cause of action for privacy invasion should be available only where there is a 'reasonable expectation of privacy'. Such a requirement would ensure that privacy is respected without unduly interfering with legitimate activities.

The LIV has previously considered that it would not be appropriate to include in any law establishing a statutory cause of action a list of matters that determine whether a given invasion is actionable. Similarly, the LIV does not consider that it would be helpful or appropriate to include a list of circumstances in which an individual would have a 'reasonable expectation of privacy'.

The LIV would, however, consider it appropriate to include some or all of these matters on a non-exhaustive basis where appropriate to guide determinations on whether there is a reasonable expectation of privacy. The following matters were suggested by the New South Wales Law

Reform Commission to be taken into account when determining whether a cause of action for an invasion of privacy arises:

- is the subject matter of the complaint private or not;
- is the nature of the invasion such as to justify an action;
- does the relationship between the parties affect actionability;
- does the claimant's public profile affect actionability;
- does the claimant's vulnerability affect actionability;
- does any other conduct of the claimant and the defendant affect actionability;
- what effect has the conduct had on the claimant; and
- does the defendant's conduct contravene a statutory provision.¹⁰

Second limb: 'Serious' invasion of privacy

The Commission is considering a statutory cause of action for 'serious' invasions of privacy. The LIV considers that this is an appropriate limit on the cause of action, as it will ensure that the resources of the justice system are not diverted by trivial invasions of privacy.

The LIV considers that the term 'serious' should not be defined in statute. It is common for legislation to limit a matter by the use of the word 'serious' but leave it to the decision-maker to determine when the threshold of 'seriousness' is reached. It would be appropriate to provide guidance to the decision-maker regarding the threshold of 'serious' by instructing a decision maker to take into account the following matters when determining whether an invasion is serious:

- the nature of the breach;
- the consequences of the invasion for an individual or individuals; and
- the extent of the invasion in terms of the numbers of individuals affected.

This is not an exhaustive list and there may be other factors that are relevant to the concept of 'serious' invasion of privacy.

Privacy and public interest

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?**

A statutory cause of action could best recognise competing public interests (such as the freedom of expression) through a defence of public interest. The defendant should carry the burden of proof to show that there is a public interest in the invasion of privacy.

Competing public interest should not be considered when determining whether there has been a serious invasion of privacy. Although competing public interests should be balanced against privacy to determine whether the defendant is liable, a person's right to privacy should not be dependent on the existence or absence of other public interests. In short, just because one person is entitled to freedom of speech does not mean that another does not have a right to privacy, but it may mean that an invasion of the person's right to privacy is not actionable.

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

Any legislation establishing a cause of action should not provide any guidance regarding the meaning of 'public interest'. This is a phrase commonly used in legislation and one with which courts are familiar. 'Public interest' is a broad concept that is flexible enough to respond to the facts

¹⁰ Clause 74(3)(a) of the NSWLRC's draft Bill lists the matters that the court must take into account in determining whether or not there has been an actionable invasion of an individual's privacy.

and circumstances of any particular case. Given that privacy is fact and context specific, it is appropriate to keep concepts such as 'public interest' broad and flexible. We note that the concept of 'public interest' is broad enough to include freedom of expression and matters of national security.

Fault

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 LIV has previously submitted that any statutory cause of action should not be limited to intention and recklessness, and should include, for example, negligence. The LIV continues to support a statutory cause of action for intentional and reckless invasions of privacy. The question of negligent invasions of privacy requires further consideration.

In past inquiries, the Commission¹¹ and the New South Wales Law Reform Commission¹² have recommended that the fault element for an invasion of privacy be limited to intentional or reckless acts. As noted in the Issues Paper released by the Department of Prime Minister and Cabinet, this is broadly consistent with the position in Canadian provinces with legislation establishing a statutory cause of action for invasion of privacy.¹³

In its inquiry into surveillance in public places, the Victoria Law Reform Commission decided that it would be unnecessary to expressly exclude negligent acts from the conduct that might fall within a statutory cause of action.¹⁴ The Victoria Law Reform Commission argued that, while it is highly likely that most serious invasions of privacy will involve intentional conduct, circumstances might arise where a person's actions are so grossly negligent that they should be civilly liable. The LIV agrees with the Victoria Law Reform Commission. We consider that it is possible that negligent invasions of privacy will occur, for example, in situations where there has been an ongoing, systematic breach or breach of individuals' privacy and the body responsible for the breach has been notified and taken no action. The LIV considered this issue in detail in its submission to the Department of Prime Minister and Cabinet:

Intentional privacy breaches, such as those alleged against News of the World in the United Kingdom,¹⁵ are not the norm. The larger threat comes from unintentional breaches caused by: a lack of understanding of privacy obligations; technological malfunction and human error; or systemic failures. This could include inadvertent dissemination of information through an Information Technology business system malfunction or a procuring government department not properly investigating a proposed Information Technology system (by independent consultants/auditors) regarding the potential of Australian data being stored on servers or databases on foreign soil. Such breaches are unlikely to be intentional or even reckless.

However, it does not follow that such failures are acceptable and should not be actionable. In the absence of a cause of action, there is little to no benefit or incentive for holders of private information in taking privacy obligations seriously. Furthermore, requiring intention, rather than

¹¹ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (August 2008), 74.165.

¹² New South Wales Law Reform Commission, *Invasion of Privacy, Consultation Paper 1* (2007), [7.24] <http://www.lawreform.lawlink.nsw.gov.au/lrc/consultpapers/LRC_cp01chp1.html>.

¹³ Commonwealth of Australia, Department of Prime Minister and Cabinet, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (September 2011), p38 <http://www.dpmc.gov.au/privacy/causeofaction/docs/issues%20paper_cth_stat_cause_action_serious_invasion_privacy.pdf>.

¹⁴ Victoria Law Reform Commission, *Surveillance in Public Places: Final Report*, Report 18 (May 2010), p152 <http://www.lawreform.vic.gov.au/sites/default/files/Surveillance_final_report.pdf>.

¹⁵ See evidence to UK House of Commons Culture, Media and Sport Committee <<http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/otherwork/phone-hacking/>>.

negligence, may be difficult to prove against companies. A cause of action must be effective in relation to companies, which have more resources and are more likely to collect, store, use and disclose large amounts of personal information.

The implications of extending a cause of action to negligence for Internet intermediaries and Internet hosts of user-generated content requires further consideration. They should be subject to any cause of action in their own right, for example protecting the information privacy of their customers and users, or not looking at what their users upload into their private accounts without lawful excuse. However, where a person is using the service as a platform and, in doing so, breaches another person's privacy, the platform should not be held liable for a breach of privacy. To do so would limit the openness of these platforms and the public interest in freedom of expression. Individual engagement in the political process should not be limited by making platforms responsible for what their users post.

We note also the limited scope of government liability for negligence. In Victoria, legislation limits the liability of public authorities for any claims for damages resulting from negligence. As a result of these limitations, it is difficult for applicants to claim damages for a breach of a statutory duty by a public authority. Some might consider it inappropriate to widen the liability of a public authority for a statutory cause of action for privacy where government liability for wrongs generally is limited. This concern can be addressed by making it clear that the statutory cause of action is not an action in negligence; rather, negligence in this context is the necessary mental element, rather than a separate cause of action in itself.

Damage

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

A statutory cause of action should not require proof of damage, consistent with the torts of trespass and defamation in Australia. The requirement of damage focuses on the effect on the plaintiff, rather than the wrong of the defendant. Some breaches of privacy will be serious, not because of their effect on an individual, but because of the scope of the breach and the number of individuals affected. Such breaches are still serious and should be actionable, as they undermine public confidence in data collection and reflect a failure on the part of a defendant to appreciate the importance of privacy protection.

If compensation for breach of privacy is to compensate for an injury to the complainant's feelings or humiliation suffered by the complainant as set out, for example, in the *Health Records Act 2001* (Vic) (section 78(1)(a)(iv)) or the *Information Privacy Act 2000* (Vic) (section 43(1)(a)(iii)), it should not be limited to damage that can be the subject of proof.

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 LIV considers that compensation should be available for 'mere distress'¹⁶ and for 'hurt, distress, embarrassment, humiliation, shame and guilt'¹⁷ caused by privacy invasions. Privacy is important because it is integral to our understanding of self and identity. The harm caused by breaches of privacy is more likely to be harm such as embarrassment, humiliation, shame and guilt. Given the centrality of privacy to identity, these harms should not be seen as insignificant, even though they are not physical or financial.

¹⁶ See e.g. in relation to a breach of confidence in *Giller v Procopets* [2008] VSCA 236, at para 431.

¹⁷ Compensation was awarded for "hurt, distress, embarrassment, humiliation, shame and guilt" in respect of breach of confidence in *Doe v. ABC & Ors* [2007] VCC 281, para 186.

Defences and exemptions

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?

The LIV would support requirements for proportionality, necessity and reasonableness. Given that privacy is a nuanced concept, requiring consideration of the surrounding facts and circumstances, absolute defences are inappropriate.

A requirement that an act be 'necessary' is insufficient to protect privacy. The Privacy Act currently requires handling of personal information to be 'necessary' for certain purposes. However, the absence of requirements for proportionality or reasonableness has permitted excessive collection, use and disclosure of personal information. For example, companies regularly use the exception of consent to collect information that is not necessary for the purpose for which it is collected (in particular, through the use of bundled consents).

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?

In Victoria, defences to defamation include truth, absolute privilege, qualified privilege and fair comment. As discussed below, the LIV believes the defences of privilege should be available for a statutory cause of action for serious invasions of privacy. We would support the defence of absolute privilege to apply, for example, to the publication of faithful and accurate reports of judicial proceedings in Victoria¹⁸ and qualified privilege to apply, for example, to statements made by a person under a legal or moral duty to another person such as information given to police about a suspected offence.

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

The LIV believes that, if an 'unreasonableness' test was introduced for serious invasions of privacy, an exhaustive list of defences may not be necessary. The LIV considers that defences to any proposed cause of action should include that the act or conduct was:

- authorised or required by law; and
- in the public interest or privileged.

With respect to acts or conduct done pursuant to law, the LIV notes that we have submitted elsewhere that certain laws should be amended to better protect privacy. A defence that an act was authorised or required by law will be an appropriate defence to the statutory cause of action only if the laws authorising or requiring the act provide adequate privacy protections. If they do not, such laws may be used to shield inappropriate invasions of privacy.¹⁹

If consent were included as a defence, it must be real, informed and proportional consent. Currently, the concept of consent is ill-defined under the Privacy Act and is much disputed. Use of bundled consent and notification masquerading as consent are used to undermine much of the protections provided in the Privacy Act.

¹⁸ See s4 of the *Wrongs Act 1958* (Vic).

¹⁹ See e.g. the LIV submission concerning draft legislation on credit reporting: <http://www.liv.asn.au/Membership/Practice-Sections/Administrative-Law---Human-Rights/Submissions/Inquiry-into-Exposure-Drafts-of-the-Australian-Pri?glist=0&rep=1&sdiag=0>.

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

The LIV does not support exemptions for particular organisations or types of organisations or types of activities. As stated above, privacy is a nuanced concept that is fact and context specific. In the circumstances, it is not appropriate to exclude specific acts or persons and absolute defences are not warranted. A defence involving the balancing of competing public interests would adequately protect legitimate activities, such as journalism or creative expression.

Current protections from invasions of privacy by media organisations are inadequate – media organisations in the course of journalism are, for example, exempt from the operation of the *Privacy Act 1988* (Cth)²⁰ – and do not provide necessary safeguards for privacy. Privacy is not anathema to, or mutually exclusive of, journalism. Neither is an absolute public interest, but must be balanced in the public interest. The current exception for media organisations is therefore inappropriate.

Monetary remedies

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 LIV has previously supported the following list of remedies for inclusion in a statutory cause of action, taken from *For Your Information: Australian Privacy Law and Practice* (Report 108).²¹

- damages, including aggravated damages, but not exemplary damages;
- an account of profits;
- an injunction;
- an order requiring the respondent to apologise to the claimant;
- a correction order;
- an order for the delivery up and destruction of material; and
- a declaration.

Notwithstanding the above, the LIV considers that exemplary damages should be available “as punishment of the guilty, to deter from any such proceeding for the future, and as a proof of the detestation [...] to the action itself”.²² It might nevertheless be appropriate to limit the amount of any award of exemplary damages.

There should be no cap on awards of damages for non-economic loss: the LIV is confident that the courts will make an appropriate assessment of damages in the circumstances of each case. However, if exemplary or ‘punitive’ damages were permitted, it might be appropriate to impose a maximum award in that instance.

The LIV notes that a court-ordered apology is not a common law remedy for defamation. Although apologies are common in settlement of defamation cases, this is often a voluntary act undertaken by the defendant. We note that the moral value of an apology compelled by legal process, as well as the question of whether compelling a defendant to publish or utter words with which he or she

²⁰ S7B9(4) of the *Privacy Act 1988* (Cth).

²¹ Australian Law Reform Commission, above n10, recommendation 74-5.

²² *Lamb v Cotogno* [1987] HCA 47; (1987) 164 CLR 1, at 8, cited in *Giller v Procopets* [2008] VSCA 236 at para 498.

does not agree is an interference with the defendant's freedom of expression, has been considered by the New South Wales Law Reform Commission.²³ The LIV acknowledges concerns among some of its members that an apology made by a defendant only because it is ordered by a court may be meaningless.

Accordingly, if an apology is to be included as an available remedy, it should be expressed as an 'apology voluntarily offered by the defendant and accepted by the plaintiff'. Such a remedy would be unlikely to arise after a contested hearing, but may be a remedy that the court can note in deciding what, if any, other remedies should be ordered.

Injunctions

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)?

As previously stated, privacy is a nuanced concept that is fact and circumstance specific. The weight to be given to any particular fact or public interest should be a matter for the court to decide on a case-by-case basis, rather than legislating the weight to be given to some public interests, but not others.

Other remedies

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

The LIV supports the remedies provided for in Recommendation 74-5 of the Commission's report *For Your Information: Australian Privacy Law and Practice* as discussed above.

Who may bring a cause of action

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?

The LIV believes living persons associated with deceased persons whose privacy has been breached should have some recourse to action. Where, for example, a deceased person's telephone messages were intercepted, a living representative of the deceased person should have recourse to civil action.

The Commission has previously considered that providing for the survival of the cause of action for the benefit of the estate of the person whose privacy was invaded before his or her death would provide acknowledgement of the harm caused by a serious invasion of privacy.²⁴ This takes into account the impact of privacy invasions on the living, particularly in Aboriginal and Torres Strait Islander cultures where strong protocols exist in relation to the publication of names and images of

²³ New South Wales Law Reform Commission, *Invasion of Privacy*, Report 120 (April 2009), p56 <http://www.lawreform.lawlink.nsw.gov.au/agdbasev7wr/lrc/documents/pdf/report_120.pdf>.

²⁴ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Issues Paper 43 (October 2013), p36.

recently deceased persons. Such provisions might also protect living relatives whose personal privacy is invaded by virtue of their connection with the deceased person.

A cause of action for defamation does not survive for the benefit of the estate in Victoria and most states of Australia, except Tasmania.²⁵ A cause of action for privacy invasions might be compared to the equitable doctrine of confidentiality, which has been considered a means of providing protection for privacy. Unlike a right to sue for defamation, a duty of confidence can persist after death.

The LIV notes that the question of whether the privacy of deceased persons should be protected is not a straightforward one and involves considerations of the relationship between privacy and a person's identity. There may be a public interest in protecting a person's identity after death. If the cause of action is to be extended to deceased persons, the remedies should be limited to those that protect the deceased's identity, for example, to allow corrective orders and declarations but not damages.

We note also the emerging issue of a deceased's online identity persisting after death. Legal questions arise in relation to who has control over a deceased person's digital account information, particularly in the context of social media.

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 LIV supports the proposal for an independent body, such as the Privacy Commissioner, to be empowered to bring actions on behalf of an individual or groups of individuals for serious invasions of privacy.

As the LIV has previously argued, empowering an independent body to bring an action on behalf of an individual or group of individuals is a means of ensuring greater access to affected individuals of limited means. This would ensure that systemic breaches, which affect large numbers of people but not in a financially significant way on an individual level, would not escape action. It would also acknowledge that privacy breaches have a public, as well as private, element. Breaches of privacy threaten the confidence individuals and the community have in transactions involving the provision or exchange of personal information.

The LIV would also support the independent body being empowered to offer services to facilitate resolution of disputes. The role of the independent body might be modelled on the dispute resolution powers granted to the Victorian Equal Opportunity and Human Rights Commission under the *Equal Opportunity Act 2010* (Vic).²⁶

The LIV considers that the Privacy Commissioner could be an appropriate body to be vested with these powers. If the Privacy Commissioner's functions and powers were extended to adjudicating complaints against individuals and providing appropriate support to unrepresented individual, the Commissioner's office should be appropriately resourced to discharge these duties.

Limitation period

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?

²⁵ Section 27 of the *Administration and Probate Act 1935* (Tas).

²⁶ See Part 8 of the *Equal Opportunity Act 2010* (Vic).

A statutory cause of action for a serious invasion of privacy should be limited to three years, consistent with causes of action for personal injuries.

Location and forum

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?

The LIV supports a statutory cause of action in Commonwealth legislation and, specifically, the Privacy Act, which should then be applied in the states and territories. We note that a person seeking information about their right of privacy will naturally look to the Privacy Act; it is logical for the cause of action to reside there.

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

The LIV notes that jurisdiction to hear cases on a statutory cause of action for serious invasions of privacy could be conferred on a range of entities including the Federal Court, the Federal Magistrates Court or State and Territory courts.

Pursuit of a claim for a breach of any statutory cause of action for serious privacy invasions in the courts will not be appropriate for some disputes: the plaintiff might not have the resources necessary to pursue a claim in court; though significant in some respect, the extent of damage or harm caused by the invasion might be small; and the time required to pursue a claim in the courts might undermine the impact that any remedy could afford.

Other options might include dispute resolution processes via an independent body (for example, the Privacy Commissioner). The LIV has previously argued that the choice of jurisdiction should provide an avenue for appropriate dispute resolution, whereby the choice of jurisdiction is appropriate to the nature and seriousness of the breach.

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

The LIV would support options for incorporating voluntary or mandatory alternative dispute resolution options into the complaints process for serious invasions of privacy. This is particularly appropriate for claims where the extent of damage or harm caused by the invasion might be small and the time required to pursue a claim in the courts might undermine the impact that any remedy could afford.

Although the LIV agrees that mandatory alternative dispute resolution is often limited in utility, it would have benefit in a privacy context, where there can be a significant power imbalance between plaintiff and defendant and where the costs of litigation could be used by a defendant to avoid liability.

Interaction with existing complaints processes

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 LIV reiterates its position that a person alleging a serious privacy invasion should have access to an administrative complaints process designed to provide them with an avenue for efficient dispute resolution. The LIV would support a provision requiring a person to access an administrative complaints process prior to pursuing the matter in a court, for example, through the responsible body's internal complaints handling process. We note that the Commission has previously reported that the most efficient means of resolving a complaint is between the complainant and respondent.²⁷ We agree with the Commission that the obligation of complaining first to the respondent should be supported by agencies and organisations adopting internal dispute resolution processes and making the avenues of complaint clear in their Privacy Policies.

Other legal remedies to prevent and redress serious invasions of privacy

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?

In the United Kingdom, privacy interests are protected under the *Protection from Harassment Act 1997*. The Act created a criminal offence for conduct that amounts to harassment of a person. The Act also creates a civil statutory tort of harassment, allowing a person to take civil proceedings in respect of harassment and empowering a court to impose civil injunctions as well as awarding damages to the victim for the harassment.

The LIV notes concerns that have been raised with the wording of the legislation, particularly that there is no complete definition of harassment. The Act has also been criticised as it does not provide for a defence of reasonableness. It has been reported that the Act has been used to curb the activities of political and other protestors and limit the right to protest.²⁸

The LIV recommends that any consideration of legislation providing for a cause of action for harassment should take into account the experience of the *Protection from Harassment Act 1997*, including the need to balance the right to freedom of privacy with other rights such as the right to freedom of expression and participation in public affairs.

²⁷ Australian Law Reform Commission, above n10, at 49.13.

²⁸ 'A-Z of the Legislation', *The Guardian* (UK), 5 November 2009
<<http://www.theguardian.com/commentisfree/libertycentral/2009/jun/01/liberty-central-protection-harassment>>
and National Council for Civil Liberties, *Your Rights: Protection from Harassment Act 1997* (9 July 2009)
<<http://www.yourrights.org.uk/yourrights/privacy/harassment-unwanted-letters-and-telephone-calls/protection-from-harassment-act-1997.shtml>>.

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 LIV has previously submitted that Victorian laws, such as the *Surveillance Devices Act 1999* (Vic), require reform to provide more comprehensive and contemporary regulation of surveillance practices.²⁹ The LIV has argued that an independent body needs to be charged and properly resourced to oversee and monitor the implementation of those laws. However the LIV reiterates that the most appropriate way to address the inadequacy of privacy laws in Victoria is to create a commonwealth statutory cause of action for invasions of privacy.

In addressing this question the Commission should consider global sensitivities to government access to personal information. Revelations of the extent of the US government's surveillance program, PRISM, and the sharing of this information with other countries sparked worldwide alarm earlier this year.³⁰ The revelations led to calls for greater transparency from government intelligence agencies. As a result, some companies and service providers now release transparency reports on the information requests received from governments. We note the Australian government rated highly on the number of requests for account information made to Apple between January 1 2013 and June 30 2013.³¹

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

The LIV notes that the advent of social media has had a significant effect on the employment relationship between employer and employee. Of concern to this Inquiry is whether employees are being subject to serious invasions of privacy by their employer or prospective employer.

The LIV holds the view that employers should not have an unfettered right to access the social media accounts of their employees or prospective employees by demanding their passwords. The LIV recognises that whilst this might be common practice in the United States, in the experience of members of the LIV's Workplace Relations Section, this practice has not made its way to Australian workplaces.

The LIV provides the following comments on privacy and social media at the various stages of the employment relationship.

Pre-employment

The LIV notes that some employers in the process of recruitment and reference checking engage in 'social media vetting' of applicants, a process whereby they search various social media platforms for information about job applicants. The information the employer recovers will be dependent on the privacy settings that the applicant has on their social media profiles.

The LIV submits that if laws were to enable an employer to request a job applicant's social media password, there is the possibility of claims of discrimination being made against the employer if the applicant is not recruited on the basis of the information contained in their social media profile. The LIV analogises providing access to a personal social media account to providing a prospective employer with keys to their home, which is considered to be unreasonable and unnecessary for the purposes of recruitment.

²⁹ LIV, *Submission to the Victorian Law Reform Commission Inquiry into Surveillance in Public Places* (6 July 2009) <<http://www.liv.asn.au/For-Lawyers/Sections-Groups-Associations/Practice-Sections/Administrative-Law-Human-Rights/Submissions/Inquiry-into-Surveillance-in-Public-Areas.aspx?rep=1&qlist=0&sdiag=0&h2=1&h1=0>>.

³⁰ See, for example, 'Ex-CIA worker Edward Snowden revealed as US spy agency whistleblower', ABC News, 10 June 2013 available at <<http://www.abc.net.au/news/2013-06-10/ex-cia-worker-revealed-as-us-spy-agency-whistleblower/4743056>>.

³¹ Apple, *Report on Government Information Requests* (5 November 2013) available at: <<http://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf>>.

During employment

The LIV submits that all employers should have a social media policy that governs acceptable usage of social media by employees. It is suggested that such policies should include issues of confidentiality. The LIV notes that there have been various cases that have arisen due to the misuse of social media with reference to and in the workplace.

The common law provides a duty that employees must comply with any 'lawful and reasonable direction' issued by their employer. As stated, the LIV strongly opposes the proposition that an employer should have an unfettered right to access their employees' social media accounts, as it cannot be considered to be a lawful and reasonable direction. On this basis, employees cannot be terminated for refusing to provide their employer with access to their social media accounts.

Post-employment

Through the use of social media platforms such as LinkedIn, the LIV acknowledges that during an employment relationship, employees are likely to have 'connected' with their employer's clients on LinkedIn.

The recent case of *Bradford Pedley v IPMS Pty Ltd T/A peckvonhartel* [2013] FWC 4282 demonstrates how social media has impacted the workplace. Pedley was employed by peckvonhartel as a senior interior designer. Pedley sent a group email via LinkedIn to a number of his employer's clients that indicated he was starting his own interior design company. His employer then terminated him after clients who received Pedley's email contacted peckvonhartel. Whilst there was no restraint of trade clause in Pedley's employment contract, the Fair Work Commission found that by sending the email, Pedley has breached his employment obligations and that the dismissal was warranted.

To avoid situations like this occurring and where restraint of trade clauses are included into employment contracts, the LIV notes that some employers are tending of late to purport to take ownership or management of LinkedIn accounts so that when employees leave, they are not taking with them what is effectively a portable client or contact list which would form part of an employer's confidential information at common law. Restraint of trade clauses operate on the basis that an employee is restricted from particular conduct once the employment relationship has ended. A former employee may be prohibited from soliciting the employer's clients and working for a similar employer for a specified period of time. In this regard, the rationale behind the prohibition is to provide employers with protection from former employees causing detriment to their business.

The need to protect against former employees poaching clients and taking confidential information from one employer to another may be the only exception as to when an employer may have a right to access an employee's social media account. However we submit that this issue is most appropriately dealt with in a workplace relations context, to be considered by employers in the construction of restraint of trade clauses in employment contracts. While the Commission should be aware of how social media impacts privacy in an employment relationship, it would not be appropriate for such situations to be specifically considered in a statutory cause of action for privacy invasions.

Other

The LIV submits that it would be useful to have national uniform workplace surveillance laws to better protect employees and give employers that operate on a national level the same standard to achieve.

Further contact

The LIV is grateful for the opportunity to provide comment on the Issues Paper and looks forward to providing further input as the inquiry progresses.