Australian Government

Australian Law Reform Commission

# Serious Invasions of Privacy in the Digital Era

ISSUES PAPER

You are invited to provide a submission or comment on this Issues Paper

Issues Paper 43 (IP 43)

October 2013

This Issues Paper reflects the law as at 26 September 2013

The Australian Law Reform Commission (ALRC) was established on 1 January 1975 by the *Law Reform Commission Act 1973* (Cth) and reconstituted by the *Australian Law Reform Commission Act 1996* (Cth).

The office of the ALRC is at Level 40 MLC Centre, 19 Martin Place, Sydney NSW 2000 Australia.

Postal Address

GPO Box 3708

Sydney NSW 2001

Telephone: within Australia (02) 8238 6333

International:+61 2 8238 6333

Facsimile: within Australia (02) 8238 6363

International:+61 2 8238 6363

E-mail: info@alrc.gov.au

Website: www.alrc.gov.au

ALRC publications are available to view or download free of charge on the ALRC website: www.alrc.gov.au/publications. If you require assistance, please contact the ALRC.

ISBN: 978-0-9873872-4-0

Commission Reference: ALRC Issues Paper 43, 2013

# Making a submission

Any public contribution to an inquiry is called a submission. The Australian Law Reform Commission seeks submissions from a broad cross-section of the community, as well as from those with a special interest in a particular inquiry.

**The closing date for submissions to this Issues Paper is 11 November 2013.**

## Online submission form

The ALRC strongly encourages online submissions directly through the ALRC website where an online submission form will allow you to respond to individual questions: www.alrc.gov.au/content/invasions-privacy-submissions-ip43 Once you have logged into the site, you will be able to save your work, edit your responses, and leave and re-enter the site as many times as you need to before lodging your final submission. You may respond to as many or as few questions as you wish. There is space at the end of the form for any additional comments.

Further instructions are available on the site. If you have any difficulties using the online submission form, please email web@alrc.gov.au, or phone +61 2 8238 6305.

Alternatively, pre-prepared submissions may be mailed, faxed or emailed, to:

The Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001
Email: privacy@alrc.gov.au
Facsimile: +61 2 8238 6363

Please send any pre-prepared submissions in Word or RTF format.

## Open inquiry policy

As submissions provide important evidence to each inquiry, it is common for the ALRC to draw upon the contents of submissions and quote from them or refer to them in publications. There is no specified format for submissions, although the questions provided in this document are intended to provide guidance for respondents.

Generally, submissions will be published on the ALRC website, unless marked confidential. Confidential submissions may still be the subject of a Freedom of Information request. In the absence of a clear indication that a submission is intended to be confidential, the ALRC will treat the submission as public. The ALRC does not publish anonymous submissions. See the ALRC policy on submissions and inquiry material for more information www.alrc.gov.au/about/policies.

# Contents

# Terms of Reference

## SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA

I, Mark Dreyfus QC MP, Attorney-General of Australia, having regard to:

- the extent and application of existing privacy statutes
- the rapid growth in capabilities and use of information, surveillance and communication technologies
- community perceptions of privacy
- relevant international standards and the desirability of consistency in laws affecting national and transnational dataflows.

REFER to the Australian Law Reform Commission for inquiry and report, pursuant to s 20(1) of *the Australian Law Reform Commission Act 1996* (Cth), the issue of prevention of and remedies for serious invasions of privacy in the digital era.

***Scope of the reference***

The ALRC should make recommendations regarding:

1. Innovative ways in which law may reduce serious invasions of privacy in the digital era.

2. The necessity of balancing the value of privacy with other fundamental values including freedom of expression and open justice.

3. The detailed legal design of a statutory cause of action for serious invasions of privacy, including not limited to:

    a. legal thresholds

    b. the effect of the implied freedom of political communication

    c. jurisdiction

    d. fault elements

    e. proof of damages

    f. defences

    g. exemptions

    h. whether there should be a maximum award of damages

    i. whether there should be a limitation period

j. whether the cause of action should be restricted to natural and living persons

k. whether any common law causes of action should be abolished

l. access to justice

m. the availability of other court ordered remedies.

4. The nature and appropriateness of any other legal remedies for redress for serious invasions of privacy.

The Commission should take into account the *For Your Information* ALRC Report (2008), relevant New South Wales and Victorian Law Reform Commission privacy reports, the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and relevant Commonwealth, State, Territory legislation, international law and case law.

***Consultation***

In undertaking this reference, the Commission will identify and consult relevant stakeholders including the Office of the Australian Information Commissioner, and relevant State and Territory bodies.

***Timeframe***

The ALRC will provide its final report to the Attorney-General by June 2014.

12 June 2013

Mark Dreyfus

Attorney-General

# Questions

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

**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?

## 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?

**Question 5.** What, if any, benefit would there be in enacting separate causes of action for:

- misuse of private information; and
- intrusion upon seclusion?

## 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?

## 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?

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

## 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?

## Damage

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

**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)?

## 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?

**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?

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

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

## 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?

## 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)?

## 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?

## 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?

**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?

## 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?

## 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?

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

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

## 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?

## 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?

**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?

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

# Issues Paper



## About the Inquiry

1. On 12 June 2013, the Attorney-General of Australia asked the Australian Law Reform Commission (ALRC) to conduct an Inquiry into ways in which the law might prevent and redress serious invasions of privacy in the digital era.

## Getting involved in the reform process

2. The ALRC will engage in widespread community and industry consultation at two stages of the Inquiry. First, the ALRC is seeking submissions addressing the questions raised in this Issues Paper (IP 43) and any other issues that stakeholders want to draw to our attention. The closing date for submissions is 11 November 2013.

3. The ALRC will then conduct consultations around the country that, along with community submissions and our own research, will assist the ALRC to formulate draft proposals for reform. These will be outlined in a Discussion Paper to be released in late February 2014. The ALRC will call for submissions on these proposals before finalising its recommendations for reform. These recommendations will be outlined in the Final Report, due at the end of June 2014.

4. Further information about ALRC consultation and submission processes—including how the ALRC uses submissions in its research and policy development work—is available on the ALRC website, along with how to subscribe to the Inquiry e-news.

## Why this Inquiry

5. The ubiquitous commercial and personal use of digital and affordable mobile technology, across all social and economic strata of society, has been world changing. New technologies allow unprecedented levels of surveillance and tracking of the activities of individuals, of recording and communication of personal information, and of intrusion into physical space. Both aspects of personal privacy that law reform commissions have previously investigated—unauthorised use of personal information and intrusion on personal privacy or seclusion—are significantly affected by the digital era and the capacities that digital technology provides.

6. This Inquiry builds on four other inquiries into privacy law or related issues conducted in Australia since 2006,[1] three of which recommended the enactment of a statutory cause of action. The divergence in these recommendations, developments in other jurisdictions, and the ever-increasing use of new technologies, makes it appropriate for further consideration to be given to the detailed legal design of a statutory cause of action in this Inquiry**.**

7. In *For Your Information; Privacy Law and Practice*, (ALRC Report 108, 2008), the ALRC recommended that Commonwealth legislation, separate from the *Privacy Act 1988* (Cth) (*Privacy Act*), should provide for a statutory cause of action for serious

1 Privacy was also the subject of earlier reports by the ALRC. In 1979, the ALRC recommended that a person be allowed to sue for damages or an injunction if 'sensitive private facts' were published in circumstances that were likely to cause distress, annoyance or embarrassment to a person in the position of the relevant individual: Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, Report No 11 (1979). In 1983, the ALRC released a report concentrating on information privacy, and the need to implement the Organisation for Economic Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data: The Australian Law Reform Commission, *Privacy*, Report No 22 (1983). This resulted in the enactment of the *Privacy Act 1988* (Cth).

invasion of privacy.[2] The recommendations set out the elements of the proposed cause of action, a range of defences, and a range of possible remedies. The section dealing with a statutory cause of action was a relatively small part of Report 108, which had a primary focus on information privacy: information collection, access or use.

8. In 2009, the New South Wales Law Reform Commission (NSWLRC) recommended that a general cause of action for invasion of privacy was required to provide a 'basis for the ongoing development of the law of privacy in a climate of dynamic societal and technological change'.[3] It also considered that the cause of action would operate to fill gaps in existing law. The NSWLRC Report included a Draft Bill.

9. In 2010, the Victorian Law Reform Commission (VLRC) issued its Report, *Surveillance in Public Places* (Report No 18), which followed a decade-long inquiry into workplace privacy and privacy in public places. The VLRC recommended separate causes of action: one for misuse of private information; and another for intrusion upon seclusion, or interference with spatial privacy.

10. Then, in September 2011, the Department of the Prime Minister and Cabinet (DPM&C) released an Issues Paper, prompted by a number of 'high profile privacy breaches' in Australia and overseas.[4] Noting the three law reform commission reports recommending an action, that Issues Paper asked a number of questions on the desirability of a statutory cause of action and on the possible elements of such an action. Approximately 80 submissions were received, from a wide range of public and private organisations and individuals, providing a very useful resource for the ALRC when deciding what issues need further consideration and what questions should be asked in this Issues Paper.

11. One factor that affects the need for, or desirability of, a statutory cause of action for invasion of privacy is the state of development of the common law protection of privacy. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, the High Court of Australia left open the possibility that a tort of invasion of privacy may develop at common law.[5] Subsequently, a tort of invasion of privacy has been recognised by two lower court decisions,[6] but no appellate court has confirmed the existence of this tort.[7]

---

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–1.

3 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 20.

4 Presumably referring to the widespread phone hacking by journalists and their sources that led to the Leveson Inquiry in the United Kingdom: Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, House of Commons Paper 779 (2012).

5 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

6 *Grosse v Purvis* [2003] QDC 151 (16 June 2003); *Doe v Australian Broadcasting Corporation* [2007] VCC 281 (2007).

7 The court in *Giller v Procopets* (2008) 24 VR 1, [168] (Ashley JA), [452] (Neave JA) found it unnecessary to consider whether the tort exists at common law. In *Sands v State of South Australia* [2013] SASC 44 (5 April 2013), Kelly J stated that 'the *ratio decidendi* of the decision in *Lenah* is that it would require a further development in the law to acknowledge the existence of a tort of privacy in Australia': [614]. In *Chan v Sellwood; Chan v Calvert* [2009] NSWSC 1335 (9 December 2009), Davies J pronounced the position on the existence of the tort at common law as 'a little unclear': [37]. *Kalaba v*

12. While the common law in Australia has not developed as quickly as some might have expected after *ABC v Lenah Game Meats*, litigants have continued to use other causes of action, such as trespass, to protect themselves from physical intrusions or the equitable action for breach of confidence to prevent unauthorised disclosure of private information.[8]

## The scope of the Inquiry

13. The Terms of Reference set out and limit the scope of the ALRC's Inquiry. In addition to making recommendations on a statutory cause of action, the ALRC is asked to make recommendations about other legal remedies and innovative ways in which the law could prevent or redress serious invasions of privacy. This will require the ALRC to consider a range of existing common law causes of action and remedies and statutory provisions, and how they might be strengthened or amended, as well as proposals for new ways in which the law could reduce or prevent invasions of privacy.

14. Submissions to previous inquiries, most recently the DPM&C Issues Paper, gave a number of reasons why the respondents favoured or opposed a statutory cause of action. The ALRC takes the view that it is not useful to ask again, in this Issues Paper, whether respondents support or oppose a statutory cause of action. The answer to that question may well depend on both the precise legal content of the statutory cause of action as proposed by the ALRC, and on the other or alternative recommendations that may be made in respect of possible ways the law could prevent or redress serious invasions of privacy. The precise form of the cause of action will have an impact on its potential interpretation and application, on the extent of protection it may provide to potential claimants, and on the activities of those who would face potential liability.

### *Balancing the value of privacy with other interests*

15. The Terms of Reference require the ALRC to make recommendations which recognise the necessity to balance the value of privacy with other fundamental values—including freedom of expression and open justice. The Inquiry considers this issue at several stages, both in relation to the enactment of a statutory cause of action and in relation to general legal remedies to prevent serious invasions of privacy. Questions 1, 7, 8 and 17 deal with this aspect of the Inquiry.

### *The detailed legal design of a statutory cause of action*

16. As the Terms of Reference set out, there are a number of important issues to be considered in the design of a statutory cause of action. Which courts or tribunals would be most appropriate to hear the action? What powers may such courts or tribunals be given under the Constitution? What sort of conduct would amount to an invasion of

---

*Commonwealth of Australia* [2004] FCA 763 (8 June 2004) found that the weight of authority was against the proposition that the tort is recognised at common law. *Gee v Burger* [2009] NSWSC 149 (13 March 2009) considered the matter 'arguable'. See also *Maynes v Casey* [2001] NSWCA 156 (2001) [35] (Basten J).

8 *TCN Channel Nine Pty Ltd v Anning* (2002) 54 NSWLR 333; *TCN Channel Nine Pty Ltd v Ilvariy Pty Ltd* (2008) 71 NSWLR 323; *Giller v Procopets* (2008) 24 VR 1; *Candy v Bauer Media Limited* [2013] NSWSC 979 (20 July 2013).

privacy? How would the claimant's rights to privacy be balanced against the defendant's rights and freedoms and other matters of public interest? How serious must an invasion of privacy be before a claimant could sue, and how would the threshold of seriousness be judged? Would the claimant have to prove that the defendant intended to invade his or her privacy, or would some lesser degree of fault be sufficient? Should a claimant have to prove that he or she has suffered some sort of damage or loss and what sort of effect should be treated as damage for this purpose? What defences should apply? Should some organisations or activities be exempt from the cause of action? How should the statutory cause of action interact with the existing regulatory and remedial framework of the *Privacy Act* and other legislation?

17. These issues are the subject of Questions 1–25 in this Issues Paper and will be a significant focus of the ALRC Inquiry.

### *Remedies and prevention of serious invasions of privacy under other existing legislation*

18. Commonwealth and state and territory privacy legislation has, since 1988, provided a wide-ranging regulatory and remedial framework for general information privacy or data protection in Australia. In addition, there is specific Commonwealth and state and territory legislation dealing with health records. The *Privacy Act* has recently been the subject of lengthy and considered review and amendment, giving the Australian Privacy Commissioner greater powers to require mandatory notification of data breaches and to require organisations to put in place or clarify their privacy policies. The amendments will take effect in March 2014 with the commencement of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) and are currently the subject of much activity in the business and governmental sectors. The ALRC does not consider it appropriate for this Inquiry to review particular aspects of Commonwealth legislation which have been the subject of recent, detailed amendment or enactment, even though they may have a considerable impact on personal privacy. This includes, for example, s 44 of the *Aviation Transport Security Act 2004* (Cth) dealing with the use of body-scanners at Australian airports.

19. Question 27 asks respondents to suggest ways in which existing legislation could be strengthened to better prevent or redress serious invasions of privacy. Respondents may wish to highlight significant gaps or inconsistencies in protection under Commonwealth, state or territory laws. However, because the ALRC is required to complete its Final Report by June 2014, its capacity to make any extensive review of existing legislation is necessarily constrained.

### *Other legal remedies and innovative ways to reduce or redress serious invasions of privacy*

20. The Terms of Reference require the ALRC to consider the nature and appropriateness of other legal remedies for serious invasions of privacy.

21. Although there is no specific common law cause of action for invasion of privacy, there are a number of common law actions which provide significant protection for individual privacy. There are, however, notable gaps in that protection.

These, and questions concerning the ways in which the existing law may be supplemented, short of a broad statutory cause of action, are discussed at Question 26.

### *Privacy in the digital era*

22. The debate about privacy in 2013 has been focused on information privacy in the digital era. In particular, attention has been given to the rapidly expanded technological capacity of organisations to track the physical location and activities of individuals, to collect and use information from social media, to aggregate data from many sources, and to intercept and interpret the details of communications. Some of these activities may amount to an invasion of the privacy of an individual. Some may breach existing criminal or civil laws or regulatory schemes on the collection or storage or dissemination of data. Comment on innovative ways in which the law may address invasions of privacy in the digital era is invited at Question 28.

23. The scope of the ALRC Inquiry extends, but is not confined, to invasions of privacy brought about by digital technology. Some gaps in the existing protection of an individual's privacy relate to physical activities or physical intrusions that fall short of the elements of existing laws such as the torts of assault or trespass to land. Question 26 addresses the issue of physical intrusions, as well as other forms of invasion of privacy.

## Principles guiding reform

24. The ALRC proposes to use the following principles to inform the development of proposals for reform. They draw on statements of principle in leading cases in Australia and other jurisdictions, international conventions, academic commentary on privacy and related fields, the Terms of Reference, and key principles identified in earlier reports, issues papers and submissions.

**Privacy as a value:** Privacy is important for individuals to live a dignified, fulfilling and autonomous life. It is an important element of the fundamental freedoms of individuals which underpin their ability to form and maintain meaningful and satisfying relationships with others; their freedom of movement and association; their ability to engage in the democratic process; their freedom to advance their own intellectual, cultural, artistic, financial and physical interests, without undue interference by others.

**Privacy as a matter of public interest:** There is a public interest in the protection of individual privacy and confidentiality.

**The balancing of privacy with other values and interests:** Privacy of an individual is not an absolute value which necessarily takes precedence over other values of public interest. It must be balanced with a range of other important values, freedoms and matters of public interest, including:

- freedom of speech, including the freedom of the media;
- freedom of artistic and creative expression;

- the proper administration of government and matters affecting the public or members of the public;
- the promotion of open justice;
- national security and safety;
- the prevention and detection of criminal and fraudulent activity;
- the effective delivery of essential services in the community;
- the protection of vulnerable persons in the community;
- national economic development and participation in the global digital economy; and
- the capacity of individuals to engage in digital communications and electronic financial and commercial transactions.

**International standards in privacy law:** The protection of privacy in Australia should be consistent with Australia's international obligations, for example, under the *International Covenant on Civil and Political Rights*, and take into account, as far as appropriate, international standards and legal developments in the protection of privacy.[9]

**Flexibility and adaptability:** The design of the legislative protection of privacy should be sufficiently flexible to adapt to rapidly changing technologies and capabilities without the need for constant amendments, but at the same time be drafted with sufficient precision and definition to promote certainty as to its application and interpretation.

**Coherence and consistency:** Any recommendation for a statutory cause of action or other remedy should promote coherence in the law and be consistent with other laws or regulatory regimes in Australian law, and should promote uniformity or consistency in the law applying throughout Australian jurisdictions.

**Access to justice:** The law should provide a range of means to prevent, reduce or redress serious invasions of privacy which provide appropriate access to justice for those affected.

**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?

9 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

# A statutory cause of action for serious invasion of privacy

## The impact of a statutory cause of action

25. Calls for a statutory cause of action for serious invasion of privacy are often made on the basis that there are gaps in existing privacy protection. These gaps may leave people who experience serious invasions of privacy with no or limited legal redress. At the same time, reservations exist about the effect of the introduction of a statutory cause of action for serious invasion of privacy. There are concerns among some stakeholders that certain worthwhile or important activities may be unduly hampered by its enactment.

26. The careful design of a statutory cause of action for serious invasion of privacy may be able to address both the expectations for, and concerns about, its impact. To begin, the ALRC is interested in hearing from stakeholders about the specific kinds of activities that a statutory cause of action for serious invasion of privacy should prevent or redress. The ALRC is particularly interested in examples of activities that the law may not already adequately prevent or redress, particularly in light of rapid technological change. The ALRC also seeks stakeholder comment on the specific activities or types of activities that the design of a statutory cause of action should be careful not to unduly hamper. The ALRC is particularly interested in specific examples of activities that may be affected in a range of business, health, community and creative sectors.

**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.

**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?

## Invasion of privacy

27. In 2008, the ALRC recommended that legislation creating a statutory cause of action should include a non-exhaustive list of examples of the types of invasions that fall within the cause of action. The ALRC considered that a serious invasion of privacy may occur where:

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;

- an individual's correspondence or private, written, oral or electronic communication has been interfered with, misused, or disclosed; or
- sensitive facts relating to an individual's private life have been disclosed.[10]

28. The ALRC seeks comment on whether such a list should be included in any Act providing for a cause of action for serious invasion of privacy, and if so, whether the list should be exhaustive or non-exhaustive. It is also interested in comment on the appropriateness of the above examples, as well as any additional examples that might be included. One issue may be whether invasions of privacy should be limited to positive conduct, and not include a failure to act.

29. An alternative approach to identifying the kinds of invasions of privacy that should be subject to legal regulation has been to develop separate causes of action relating to specific categories of invasions of privacy—principally, the torts of misuse of private information and intrusion upon seclusion.[11]

30. The VLRC took this course in recommending that two causes of action for invasion of privacy be enacted. The two causes of action were to deal with misuse of private information and intrusion upon seclusion—or interference with spatial privacy—respectively. The VLRC argued that enacting two causes of action, rather than a general cause of action for invasion of privacy, was 'likely to promote greater clarity about the precise nature of legal rights and obligations that have been created'.[12]

31. Disadvantages of multiple causes of action may be that there could be overlap between them, and that some invasions of privacy may not be captured by either cause of action. The ALRC is interested in hearing from stakeholders about the desirability of separate causes of action for the two different types of 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?

---

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–1.

11 The UK has recognised a cause of action for invasion of privacy in respect of misuse of private information, which some judges have described as a tort: *Campbell v MGN Ltd* [2004] 2 AC 457, [14]; *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [27]. New Zealand (NZ) courts have recognised a tort of misuse of private information and a tort of intrusion upon seclusion: *Hosking v Runting* (2005) 1 NZLR 1; *C v Holland* [2012] NZHC 2155 (24 August 2012). In the US, two additional torts have developed: the appropriation to one's use or benefit of another's name or likeness; and giving publicity to a matter concerning another that places a person in a false light: American Law Institute, *Restatement (Second) of Torts* (1977) §§ 652B–652E. It is arguable that the additional US torts should not be characterised as invasions of privacy and are better dealt with in Australian law through intellectual property, the tort of passing off, or defamation: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2566.

12 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 149.

**Question 5** What, if any, benefit would there be in enacting separate causes of action for:

- misuse of private information; and
- intrusion upon seclusion?

## Privacy and the threshold of seriousness

32. Two main issues arise for consideration when developing the test for serious invasion of privacy. The first is the circumstances in which the privacy violation is said to have occurred. The second is determining the degree of seriousness of an invasion of privacy.

### *What is 'private'?*

33. For an invasion of privacy to occur, there must be a violation of circumstances that can be considered 'private'. In *ABC v Lenah Game Meats*, Gleeson CJ observed that there is no 'bright line' between what may be considered legitimately private and public, noting that:

> there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public … Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved.[13]

34. The ALRC, NSWLRC and VLRC have all previously recommended that the test of whether a matter is private is that there exists a reasonable expectation of privacy in the circumstances.[14] This test is also used in a number of other jurisdictions.[15]

### *Threshold of seriousness*

35. It may be appropriate to qualify the 'reasonable expectation' test by including an additional threshold test of 'seriousness' before an invasion of privacy is actionable. An additional test of seriousness may be appropriate to discourage litigation of trivial

---

13 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–2; Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 25, 26; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 24.

15 For example, the United Kingdom, Canada and New Zealand: 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, DPM&C, 2011) 17–21. In the United Kingdom, Lord Hope in the majority in *Campbell v MGN Ltd* stated that 'the question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity': [2004] 2 AC 457, [99]. The 'reasonable expectation of privacy' test is also used in the United States when considering possible violations of Fourth Amendment privacy rights: *Katz v United States* 389 US 347, 360, 361 (1967).

or minor matters.[16] For example, the ALRC and VLRC recommended that, in addition to establishing a reasonable expectation of privacy, a plaintiff also be required to show that the act or conduct complained of was highly offensive to a reasonable person of ordinary sensibilities.[17] It is recognised that the highly offensive test is more stringent than the reasonable expectation of privacy test alone.[18]

36. A 'highly offensive' test may not be the most appropriate way to identify seriousness for the purposes of a statutory cause of action for serious invasion of privacy. It may be that this test sets the threshold too high for an actionable serious invasion of privacy, discouraging otherwise meritorious claims.[19] Possible alternatives include that the invasion 'caused substantial offence',[20] or was 'sufficiently serious to cause substantial offence'[21] to a reasonable person of ordinary sensibilities.

37. It may also be argued that 'offensiveness' is not an appropriate test of seriousness. Possible alternatives to offensiveness as a test of seriousness include that the act or conduct was likely to cause substantial or serious 'distress' or 'harm'.[22] It is also arguable that simply requiring that the invasion was 'serious' would be sufficient.[23]

38. Others suggest that the invasion of the privacy a person is reasonably entitled to expect is alone a sufficient test for an actionable invasion.[24]

---

16 See, eg, Free TV Australia, Submission No 10 to DPM&C Issues Paper, 2011; SBS, Submission No 8 to DPM&C Issues Paper, 2011.

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–2; Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 25, 26. It is worth noting that the 'highly offensive' test is at times conceptualised as going to the seriousness of an invasion and, at others, as a test of what may be considered private. An example of the latter is Gleeson CJ's statement in *ABC v Lenah Game Meats* that 'the requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private': (2001) 208 CLR 199, [42].

18 *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [25]–[26].

19 Office of the Australian Information Commissioner, Submission No 14 to DPM&C Issues Paper, 2011; Australian Privacy Foundation, Submission No 7 to DPM&C Issues Paper, 2011.

20 Liberty Victoria, Submission No 34 to DPM&C Issues Paper, 2011.

21 Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) Prop 5–2.

22 For example, the *Defamation Act 2013* c 26 (UK) provides that a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant: s 1.

23 From 12 March 2014, the *Privacy Act 1988* (Cth) will introduce civil penalties for 'serious' interferences with the privacy of individuals: *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 4 cl 50. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) states that 'serious' will not be defined, and that its ordinary meaning will apply.

24 For example, the NSWLRC considered that there should be no additional threshold for invasion of privacy beyond the reasonable expectation of privacy test. The nature of the conduct comprising the invasion, and the offensiveness of such conduct, were instead matters to be taken into account when determining whether an actionable invasion of privacy had occurred: NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 23–33.

**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?

## Privacy and public interest

39. A key question for this Inquiry will be how best to balance the public interest in the protection of privacy with competing public interests, including, but not limited to, freedom of expression.[25]

40. Privacy may be balanced with other public interests by requiring that other interests must be considered as part of the cause of action.[26] Alternatively, the balancing may be achieved by including a public interest defence to the cause of action.[27]

41. If the balancing between privacy and other public interests is to be integrated with the cause of action, there is a further question of precisely when and how the balancing is to occur.

42. The NSWLRC has argued that the consideration of competing public interests will often occur as part of the inquiry into whether or not a plaintiff had a reasonable expectation of privacy in the circumstances. It argued that the two issues of whether or not a matter is legitimately private, and the significance of competing interests,

> are not always clearly separable. Thus, a competing public interest may be of such force in the circumstances that the case will focus principally on it in reaching a conclusion that no reasonable expectation of privacy arises.[28]

43. A different approach to the balancing of interests is taken in the United Kingdom (UK).[29] There, a two-stage approach is required in determining whether the cause of action for misuse of private information has been established:

---

25 Setting a high threshold for a serious invasion of privacy may also go some way to 'ensure that freedom of expression is respected and not unduly curtailed': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2568.

26 The ALRC and NSWLRC supported this approach: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 74–2; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 31–32. The ALRC recommended that, as an additional element of the cause of action, the court must consider whether 'the public interest in maintaining the claimant's privacy outweighs other matters of public interest'.

27 The VLRC supported this approach: Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 27, 28.

28 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 63.

29 This approach is informed by the UK's incorporation into domestic law of the right to privacy and to freedom of expression contained in arts 8 and 10 of the European Convention on Human Rights: *European Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953); *Human Rights Act 1998* (UK).

> First, is the information private in the sense that it is in principle protected by article 8? If no that is the end of the case. If yes, the second question arises: in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by article 10?[30]

44. Alternatively, it may be more appropriate for public interest to be a defence than to be considered as part of establishing the cause of action. New Zealand provides a defence of 'legitimate public concern' to invasions of privacy.[31] Where the act of invasion was a publication, the four Canadian provinces that have enacted statutory causes of action for invasion of privacy provide a defence where the publication was in the public interest.[32] The VLRC also recommended that public interest should properly be considered as a defence to invasions of privacy.[33]

### *The onus of proof*

45. The location of the public interest balancing exercise will have an impact on the onus of proof. The VLRC based its recommendation that public interest should be a defence to an invasion of privacy largely upon its assessment that the burden of proving the existence of a countervailing public interest should lie with the defendant. It argued that a plaintiff 'should not have to prove a negative, such as the lack of a countervailing public interest'.[34]

46. In contrast, the NSWLRC considered that the onus of proof in relation to public interest should lie with the plaintiff. It contended that 'it is appropriate … that, as part of establishing an invasion of privacy, plaintiffs should demonstrate at the outset that their claim to privacy is not outweighed by a competing public interest'.[35]

47. Dr Normann Witzleb has suggested that the question of who bears the onus of proof may not have significant practical implications. Where public interest considerations are considered as part of establishing the cause of action, Witzleb considers that this

> will, in many cases, prompt the plaintiff to provide evidence that is relevant to the public interest considerations in the balancing process. In practice, however, the defendant will often be in a better position, and have the greater interest, to adduce the evidence necessary for establishing the weight of the public interest in his or her conduct.[36]

### *How should public interest be understood?*

48. The ALRC is interested in stakeholder comment as to whether any guidance should be provided on the meaning of 'public interest' for the purposes of a statutory

---

30 *McKennitt v Ash* [2008] 1 QB 73, [11].

31 In relation to the publication of private information, see: *Hosking v Runting* (2005) 1 NZLR 1, [129]. In relation to intrusion upon seclusion, see: *C v Holland* [2012] NZHC 2155 (24 August 2012) [96].

32 See, eg, *Privacy Act* RSBC 1996 c 373 s 2(3)(a).

33 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 156–158.

34 Ibid 157.

35 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 33.

36 Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' [2011] *Torts Law Journal Lexis 6* [49].

cause of action. Such guidance might include, for example, a definition of public interest, or a list of examples of relevant matters of public interest.[37] Guidance may assist in providing clarity and certainty about what is meant by 'public interest'. Matters of public interest may include those identified in the guiding principles for the Inquiry.

49. On the other hand, it may be more appropriate to leave public interest undefined. In the UK, the Joint Committee on Privacy and Injunctions concluded that there should not be a statutory definition of the public interest, 'as the decision of where the public interest lies in a particular case is a matter of judgment, and is best taken by the courts in privacy cases'.[38] In *Hogan v Hinch*, French CJ stated that, when 'used in a statute, the term [public interest] derives its content from "the subject matter and the scope and purpose" of the enactment in which it appears'.[39]

**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?

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

## Fault

50. A key element in any cause of action leading to a personal liability to pay compensation for loss or damage caused to another person[40] is the fault element, or in the absence of a fault element, a strict liability.

51. The term 'fault' in a civil cause of action refers to either the state of mind of the relevant actor or the culpability of the actor's conduct on an objective measure. Torts, or other bases of liability, such as statutory liabilities or liabilities for breaches of equitable duties, tend to be divided into actions imposing fault-based liability or actions imposing strict liability. Fault is generally comprised of either an actor's intent to bring about the relevant interference with the plaintiff or the plaintiff's interests, or the actor's negligence in causing that interference. Conduct may be considered as

37 For example, the Australian Press Council defines public interest as 'involving a matter capable of affecting the people at large so they might be legitimately interested in, or concerned about, what is going on, or what may happen to them or to others': Australian Press Council, *General Statement of Principles* <www.presscouncil.org.au/general-principles/>.

38 Joint Committee on Privacy and Injunctions, *Privacy and Injunctions*, House of Lords Paper No 273, House of Commons Paper No 1443, Session 2010–12 (2012) 19.

39 (2011) 243 CLR 506, [31].

40 Liability to pay compensation or make amends to a claimant in a civil action must be distinguished from the consequences of a breach of a regulatory scheme such as the *Privacy Act 1988* (Cth) which may flow regardless of whether loss or damage has been caused by the breach.

intentional or satisfying the requirement for intention where it involves a high degree of recklessness.[41] Negligence depends on whether the actor's conduct measured up to an objective standard of what a reasonable person would do or not do in the circumstances.

52. Strict liability is liability that is imposed without the need for the claimant to prove any fault on the part of the defendant. Instances of strict liability are now relatively rare in Australian common law outside contractual obligations and fiduciary obligations, both of which rest on relationships that, ordinarily, have been voluntarily entered into by the parties. In *Northern Territory v Mengel*, a majority of the High Court remarked that

> the recent trend of legal development, here and in other common law countries, has been to the effect that liability in tort depends on either the intentional or the negligent infliction of harm. That is not a statement of law but a description of the general trend.[42]

53. Defamation is one of the rare examples of a common law tort liability that is strict, and is complete on proof of publication of defamatory material identifying the claimant. The uniform *Defamation Acts* enacted in the Australian states in 2005 provide for a defence of innocent dissemination.[43] Another example is the tort action for breach of a statutory duty where the duty imposed by the statute is strict. Most strict liabilities now arise by statute. Important examples in Australian law are:

- the statutory liability for losses caused by breach of the prohibition of misleading or deceptive conduct in trade or commerce imposed by the *Australian Consumer Law* and state *Fair Trading Acts*;[44]
- statutory liabilities for damage caused by defective products;[45] and
- the liability imposed by legislation for damage caused by aircraft.[46]

54. Previous law reform reports have diverged on the issue of fault. The ALRC recommended that liability should be limited to intentional or reckless conduct, with 'intentional' defined as being where the defendant 'deliberately or wilfully invades the plaintiff's privacy' and 'reckless' having the same meaning as in s 5.4 of the *Criminal Code* (Cth).[47] The ALRC agreed with what had been said in the NSWLRC Consultation Paper in 2007, that 'including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[48] Neither the

---

41 *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417, [80] (Spigelman CJ).

42 (1995) 185 CLR 307, [341–342] (Mason CJ, Dawson, Toohey, Gaudron and McHugh JJ).

43 See, eg, *Defamation Act 2005* (Qld) s 32.

44 *Competition and Consumer Act 2010* (Cth) sch 2 s 236. Each state and territory *Fair Trading Act* applies the Australian Consumer Law as a law of its jurisdiction: see, eg, *Fair Trading Act 1987* (NSW) s 28.

45 *Competition and Consumer Act 2010* (Cth) sch 2 ss 138–141.

46 See, eg, *Damage by Aircraft Act 1999* (Cth) s 10.

47 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2576.

48 Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) 2577; NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007) 171.

NSWLRC nor the VLRC recommended a fault element as part of the recommended cause or causes of action, but the NSWLRC recommended a defence of innocent dissemination similar to that found in the *Defamation Acts*.[49]

55. Submissions to the DPM&C Issues Paper show a range of views on the issue of whether, and what, degree of fault should be required for an invasion of privacy to be actionable. Only a very small number favoured strict liability, arguing that fault should be relevant only to damages or that reasonable care should be a defence.[50]

56. A number of submissions favoured requiring at least a degree of intent or recklessness.[51] Some of these further noted that the relevant intent should be the intent to invade the privacy of the plaintiff and not merely an intent to do an act which invades the privacy of the plaintiff.[52]

57. Other submissions argued that negligent invasion of privacy should be sufficient fault, some noting that an invasion of privacy may arise out of a systemic failure,[53] but most arguing that liability should be imposed only where the negligence was gross or serious.[54]

58. A number of submissions linked the fault requirement with the issue of whether damage is required. It can be inferred that they were concerned that a person could be strictly liable even if the action were actionable *per se*, that is, without proof of damage.[55]

> **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?

## Damage

59. The ALRC has previously recommended that a statutory cause of action for invasions of privacy should be actionable without proof of damage.[56] The NSWLRC

---

49 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 55.

50 See, eg, Office of the Privacy Commissioner NSW, Submission No 79 to DPM&C Issues Paper, 2011; Maurice Blackburn Lawyers, Submission No 45 to DPM&C Issues Paper, 2011.

51 See, eg, Liberty Victoria, Submission No 34 to DPM&C Issues Paper, 2011; ABC, Submission No 18 to DPM&C Issues Paper, 2011.

52 Arts Law Centre of Australia, Submission No 15 to DPM&C Issues Paper, 2011.

53 This issue is discussed further below when considering remedies for a statutory cause of action for serious invasion of privacy.

54 See, eg, Law Institute of Victoria, Submission No 67 to DPM&C Issues Paper, 2011; Public Interest Advocacy Centre, Submission No 59 to DPM&C Issues Paper, 2011; Law Society of New South Wales, Submission No 51 to DPM&C Issues Paper, 2011; Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011.

55 Associate Professor David Rolph, Submission No 73 to DPM&C Issues Paper, 2011; Peter A Clarke, Submission No 69 to DPM&C Issues Paper, 2011.

56 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–3.

and VLRC proposals also did not require proof of damage for an invasion of privacy to be actionable.

60. Such an approach would make invasions of privacy akin to intentional torts such as trespass and would be 'recognition that the cause of action protects a fundamental human right'.[57] It also recognises that invasions of privacy are often non-financial in consequence or may result in distress, humiliation and insult that fall short of provable damage.[58] It would also allow the court to award a wider range of remedies to redress the invasion of privacy, such as an order requiring the defendant to apologise to the plaintiff.[59]

61. However there is a concern that making the statutory cause of action actionable *per se* would encourage a proliferation of claims[60] and may lead to significant extra costs to industry.[61]

62. A middle ground between making the cause of action actionable *per se* and making it depend on proof of damage may be found by including the suffering of humiliation or emotional distress within the definition of 'damage' for the purposes of the cause of action.[62] This would be consistent with s 52 of the *Privacy Act 1988* (Cth), which currently provides that the loss or damage resulting from an interference with the privacy of an individual, as to which the Privacy Commissioner may make a determination of an entitlement to compensation or other remedy, 'includes injury to the complainant's feelings or humiliation suffered by the complainant'.

63. As is noted below, at paragraph 162, the inability of the common law to award damages in tort for emotional distress, even where it is intentionally inflicted, unless the circumstances amount to a trespass or defamation, is one of the key gaps in the common law's redress for conduct invading privacy.[63] The position in the equitable action for breach of confidence in Australia could still be regarded as somewhat uncertain, given the paucity of authority.[64]

---

57 Ibid 2577.

58 NSW Council for Civil Liberties, Submission No 62 to DPM&C Issues Paper, 2011; Public Interest Advocacy Centre, Submission No 59 to DPM&C Issues Paper, 2011.

59 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2577.

60 Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011; SBS, Submission No 8 to DPM&C Issues Paper, 2011. The concern as to a proliferation of claims may be answered by the threshold requirements for actionability discussed above. Concerns about a large number of unmeritorious claims may also be reduced if fault were required for actionability.

61 Australian Direct Marketing Association, Submission No 57 to DPM&C Issues Paper, 2011.

62 If negligence was to be included as sufficient fault for the cause of action, the compatibility of any such provision with the provisions of state *Civil Liability Acts* requiring a recognised psychiatric illness for actionability of negligent conduct would need to be considered. See, eg, *Civil Liability Act 2002* (NSW) ss 29, 31; *Civil Liability Act 2002* (WA) s 5T; *Civil Liability Act 2002* (Tas) s 33.

63 *Wilkinson v Downton* [1897] 2 QB 57 discussed in *Giller v Procopets* (2008) 24 VR 1; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.

64 Damages for mental distress have been awarded in the United Kingdom for breach of confidence since the enactment of the *Human Rights Act 1998* (UK): see, eg, *Campbell v Mirror Group Newspapers* [2002] EWHC (QB) 499. They were awarded in the Victorian Court of Appeal in the equitable action for breach of confidence: *Giller v Procopets* (2008) 24 VR 1.

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

**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)?

## Defences and exemptions

### *Defences*

64. To some extent, the appropriate defences to a serious invasion of privacy will depend on the elements of the statutory cause of action. For example, if a consideration of public interest occurs as one of the elements of the cause of action, then a defence of public interest is unnecessary. Similarly, it is arguable that consent should be relevant to considering whether the threshold for a serious invasion of privacy has been established, rather than as a defence.[65]

65. A defence to the statutory cause of action that the act or conduct was required or authorised by or under law was uniformly recommended by the ALRC, NSWLRC and VLRC.[66]

66. Another defence might be that the act or conduct was 'incidental to the exercise', or 'for the purpose' of, a lawful right of defence of person or property.[67] The VLRC suggested that such a defence may be relevant to conduct including 'an employer taking privacy invasive action to prevent employee pilferage of stock … [and] conduct undertaken for the purpose of prosecuting or defending civil or criminal proceedings, such as private investigations'.[68]

67. The ALRC seeks stakeholder comment as to whether this is an appropriate defence to the statutory cause of action and, if so, whether it should be qualified by a

---

65 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2575–2576. By contrast, the VLRC concluded that consent should be a defence: Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 27, 28.

66 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–4; Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 27, 28; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 52. The defence is also available to a statutory cause of action for invasion of privacy in four Canadian provinces: see, eg, *Privacy Act* RSBC 1996, c 373, s 2(2)(c). The ALRC expressed the view that, in relation to this defence, 'law' should include 'Commonwealth and state and territory Acts and delegated legislation as well as duties of confidentiality under common law or equity': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2578.

67 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–4; Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Recs 27, 28; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 51.

68 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 154.

requirement that the act or conduct was proportionate, or necessary and reasonable. Without this qualification, such a defence may provide protection for conduct that goes beyond what might be appropriate to safeguard persons or property in a particular instance.[69]

**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?

68. It may also be appropriate that defences similar to those available for defamation should be included as defences to a statutory cause of action for serious invasion of privacy. Such defences would be relevant where the invasion of privacy involved the publication of private facts or information. In particular, the defences to defamation of absolute or qualified privilege may be considered to be suitable defences to a statutory cause of action for serious invasion of privacy.

69. Absolute privilege will attach to any statement made on a 'privileged occasion': principally, where a matter is published in the course of the proceedings of a parliamentary body, or of an Australian court or Australian tribunal.[70]

70. Qualified privilege, in state and territory defamation legislation, will apply where:

- the recipient of the information has an interest, or apparent interest, in having information on some subject; and
- the matter is published to the recipient in the course of giving to the recipient information on that subject; and
- the conduct of the defendant in publishing that matter is reasonable in the circumstances.[71]

71. Qualified privilege is also a common law defence to defamation. The common law has recognised four broad categories protected by qualified privilege:

- publication of material in the performance of a duty or to protect an interest;
- communications concerning government and political matters;
- fair reports of judicial and parliamentary proceedings; and
- extracts from public records, if they are part of a register kept pursuant to legislation that, by the legislation, is open to public inspection.[72]

---

69 Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' [2011] *Torts Law Journal Lexis 6*, [64].

70 See, eg, *Defamation Act 2005* (Qld) s 27(2).

71 See, eg, ibid s 30(1).

72 Westlaw, *The Laws of Australia* (at 1 January 2013) 6 Communications, '6.1.7 Civil Defamation Defences' [6.1.1370], [6.1.1470]–[6.1.1490].

72. The defence of qualified privilege concerning government and political matters may be particularly relevant to ensuring that a statutory cause of action for serious invasion of privacy does not infringe upon the implied constitutional freedom of political communication.[73]

**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?

73. Other appropriate defences to a statutory cause of action for serious invasion of privacy may include defences that:

- there is another remedy available in respect of the invasion of privacy;[74]
- the information was already in the public domain;[75]
- the disclosure of information was made for the purpose of rebutting an untruth;[76]
- the circumstances justified the conduct as a matter of necessity;[77]
- there was a contractual waiver;
- for online material, that the material has been taken down upon notification.[78]

74. The ALRC seeks stakeholder comment on what defences should be available to a statutory cause of action for serious invasion of privacy. It is particularly interested in defences that may be appropriate for internet intermediaries or internet sites hosting material posted by third parties.

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

### *Exemptions*

75. It may be appropriate for certain activities or functions to be exempt from the ambit of a statutory cause of action. On the other hand, it may be argued that the defences to the statutory cause of action provide sufficient protection for persons

---

73 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

74 SBS, Submission No 8 to DPM&C Issues Paper, 2011.

75 Free TV Australia, Submission No 10 to DPM&C Issues Paper, 2011.

76 Media, Entertainment and Arts Alliance, Submission No 78 to DPM&C Issues Paper, 2011; Optus, Submission No 64 to DPM&C Issues Paper, 2011. Free TV Australia, Submission No 10 to DPM&C Issues Paper, 2011.

77 Patrick George, Submission No 31 to DPM&C Issues Paper, 2011.

78 Australian Direct Marketing Association, Submission No 57 to DPM&C Issues Paper, 2011. Such a defence might have similarities to the 'safe harbours' in div 2AA of the *Copyright Act 1968* (Cth), or sch 5 cl 91 of the *Broadcasting Services Act 1992* (Cth).

'engaged in legitimate activities from unmeritorious actions for serious invasion of privacy'.[79]

76. The DPM&C Issues Paper suggested that there may be a need for national security and law enforcement agencies to be exempted from the ambit of a statutory cause of action for serious invasion of privacy. A number of factors may justify such an exemption, including that:

- such agencies are already subject to internal or legislative oversight and integrity mechanisms;
- law enforcement and intelligence gathering activities have particular characteristics that make exposure to liability for a statutory cause of action inappropriate; and
- a public interest exists in enforcement of criminal law and national security.[80]

77. Other organisations, services or functions that stakeholders have proposed to be exempted included emergency services and social support services;[81] journalists;[82] banks;[83] Commissions of Inquiry; and the exercise of judicial functions.[84]

78. It has also been argued that there should be an exemption for providers of social networking platforms or other internet sites with respect to material posted by third parties.[85]

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

## Monetary remedies

79. The main monetary remedies that are likely to be available for a breach of the statutory cause of action for serious invasion of privacy are damages and an account of profits.

### *Damages*

80. The ALRC seeks stakeholder comment on the kinds of damages that should be available for serious invasion of privacy, as well as any restrictions on such damages.

---

79 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 160.

80 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, 2011) 43–44.

81 Support Link, Submission No 28 to DPM&C Issues Paper, 2011.

82 See, eg, Commercial Radio Australia, Submission No 27 to DPM&C Issues Paper, 2011; Free TV Australia, Submission No 10 to DPM&C Issues Paper, 2011; SBS, Submission No 8 to DPM&C Issues Paper, 2011.

83 Australian Bankers' Association, Submission No 72 to DPM&C Issues Paper, 2011.

84 Office of the Information Commissioner, Queensland, Submission No 1 to DPM&C Issues Paper, 2011.

85 Peter Leonard and Michael Burnett, Submission No 77 to DPM&C Issues Paper, 2011. Leonard and Burnett suggest that a useful model for such an exemption exists in the *Broadcasting Services Act 1992* (Cth) sch 5 cl 91.

81. In tort, the object of damages is to compensate the plaintiff. The award of damages seeks to place plaintiffs, as far as possible, in the position they would have been in had the wrong not been committed.[86] Aggravated damages may be awarded to further compensate the plaintiff where the defendant's conduct aggravates or intensifies the injury done to the plaintiff, causing, for example, particular insult or humiliation.[87]

82. Exemplary damages are punitive in nature and may be awarded to mark the court's disapproval of the defendant's actions.[88] Previous reports have recommended that damages awarded for serious invasions of privacy should include compensatory damages, but not include exemplary damages.[89] However, it may be argued that exemplary damages should be available for malicious or egregious invasions of privacy.[90]

83. In certain circumstances it may be appropriate for the defendant who has invaded the privacy of an individual to pay damages based on the assessment of a 'notional licence fee'. This fee would compensate the individual whose privacy has been seriously invaded for any income that the individual would have received if the defendant had been required to pay a fee to carry out the activity that invaded the plaintiff's privacy.[91]

84. In the context of serious invasions of privacy, a notional licence fee may be an appropriate remedy where, for example, there has been publication of privacy-invasive photographs. The plaintiff in such a case might receive a 'notional licence fee' equal to the amount that would have been received had the plaintiff sold the photograph.[92] While a notional licence fee generally arises due to commercial interests rather than privacy interests,[93] it may nevertheless be an appropriate remedy in cases where both privacy and commercial interests are concerned. It may also provide an appropriate

---

86 Westlaw, *The Laws of Australia* (at 3 August 2007) 33 Torts, '33.10 Damages' [33.10.10].

87 Ibid [33.10.180].

88 Ibid [33.10.190].

89 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–5; Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Rec 29. The NSWLRC recommended that compensation orders be payable, but that aggravated damages not be available for the statutory cause of action: NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 58–60.

90 Public Interest Advocacy Centre, Submission No 59 to DPM&C Issues Paper, 2011; Law Council of Australia, Submission No 55 to DPM&C Issues Paper, 2011; Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011.

91 For example, in *Irvine v Talksport*, a radio station used the image of a well-known racing driver in its publicity material, without the driver's knowledge or agreement. The court granted the driver damages equal to the driver's minimum endorsement fee at the time the image was used: [2003] 2 All ER 881.

92 For example, in *Douglas v Hello!*, the court considered whether to award damages based on a notional licence fee when unauthorised photographs of the claimants' wedding were published by a magazine that was a rival to the magazine that published authorised photographs of the wedding. Ultimately, however, a notional licence fee was not granted, since the claimants would not have agreed to license their photographs to the defendant and, moreover, they would not have been in a position to do so given their existing licence with the defendant's rival: [2005] EWCA (Civ) 595 (18 May 2005).

93 See, eg, *Wrotham Park Estate Co Ltd v Parkside Homes Ltd* [1974] 1 WLR 798; *Experience Hendrix Llc v Times Newspapers Ltd* [2010] EWHC (Ch) 1986 (30 July 2010).

remedy where the laws of passing off would not be available to the plaintiff because the plaintiff lacked goodwill or a commercial reputation.[94]

85. It may be considered appropriate to place a cap on the maximum award of damages—either in total, or for non-economic loss—that can be made for a serious invasion of privacy. For example, a cap could be set in line with, or lower than, that for defamation.[95] Some stakeholders have argued that such a limit would discourage 'forum shopping' between causes of action.[96] Others contend that no cap is necessary, citing the likelihood that modest sums will be awarded for serious invasions of privacy;[97] and the risk that, if set too low, damages would not act as an effective deterrent for serious invasions of privacy.[98]

### *Accounts of profit*

86. An account of profits is an equitable remedy that may be granted in cases where a defendant has profited from a wrongful action. It is distinct from an award of damages in that it responds to the gain of the wrongdoer rather than the loss of the party wronged. An account of profits is a possible remedy for breaches of confidence[99] and breaches of fiduciary duty.[100] It is also available for infringement of copyright.[101]

87. Although there may be many serious invasions of privacy that do not lead to profits for the wrongdoer, there may be many other serious invasions that do. An unauthorised photograph of a celebrity in their home that is sold to a magazine is one obvious example; another is an employee of a company who accesses a customer's personal information without authorisation for personal gain.

88. An account of profits was recommended as a remedy for a serious invasion of privacy by the ALRC and NSWLRC.[102] Both Commissions noted the concerns of some stakeholders that in many cases it would be difficult to determine the profits arising from a serious invasion of privacy, but neither considered that this should preclude an account of profits being available.

---

94 *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd* [1981] 1 NSWLR 196 204; R P Balkin and JLR Davis, *Law of Torts* (Butterworth Law, 4th ed, 2009) 676–680.

95 The maximum amount of damages for non-economic loss that may be awarded in defamation proceedings is $250,000: see, eg, *Defamation Act 2005* (Qld) s 35(1). An order exceeding the maximum amount may be made if the court is satisfied that aggravated damages are warranted: see, eg, Ibid s 35(2).

96 Australian Bankers' Association, Submission No 72 to DPM&C Issues Paper, 2011; Law Society of New South Wales, Submission No 51 to DPM&C Issues Paper, 2011; ABC, Submission No 18 to DPM&C Issues Paper, 2011.

97 See, eg, Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 161; Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011.

98 Public Interest Advocacy Centre, Submission No 59 to DPM&C Issues Paper, 2011.

99 *Peter Pan Manufacturing Corporation v Corsets Silhouette Ltd* [1964] 1 WLR 96; *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109.

100 *Warman International Ltd v Dwyer* (1995) 182 CLR 544.

101 See, eg, *Copyright Act 1968* (Cth) s 115.

102 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–5; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 66.

**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?

## Injunctions

89. An interlocutory injunction is the most significant remedy to prevent a threatened invasion of privacy, such as the in-print, broadcast or online publication of private information. As with all court orders, its efficacy will depend on the jurisdiction of the court over the apprehended conduct and the location of the respondent. The court will not grant an injunction where it would be futile to do so.[103]

90. Of all remedies, an interlocutory injunction restraining publication is also the most significant restriction on freedom of speech and freedom of the media to report on matters of public interest and concern. By the time the basis for the interlocutory injunction is adjudicated in a final hearing, the opportunity to reveal the relevant information at the appropriate time may have been lost or overtaken by other events.

91. The Terms of Reference of this Inquiry direct the ALRC to make recommendations as to the necessity to balance the value of privacy with other fundamental values including freedom of expression and open justice. One way the ALRC might do this is by making specific recommendations with regard to the matters that a court should take into account when considering the award of an injunction. Such a recommendation might be made with respect to both a statutory cause of action and existing causes of action.

92. According to equitable principles, before the court will exercise its discretion to award an injunction, an applicant for an interlocutory injunction has to satisfy the court that:

- there is a serious question to be tried as to the plaintiff's entitlement to relief;
- the plaintiff is likely to suffer injury for which damages will not be an adequate remedy; and
- the balance of convenience favours the granting of an injunction.[104]

---

103 *Candy v Bauer Media Limited* [2013] NSWSC 979 (20 July 2013) [20]; *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, 428–29.

104 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [19].

93. In actions for defamation, an applicant faces additional hurdles when seeking an interlocutory injunction.[105] In *ABC v O'Neill*, Gleeson CJ and Crennan J noted that, in defamation cases, particular attention will be given to the public interest in free speech when considering whether an interlocutory injunction should be granted.[106]

94. Privacy cases raise somewhat different issues from defamation cases, because, in a privacy case, a defendant cannot depend on the truth of the disclosed information as a defence.[107] Nevertheless, there is a similar concern with undue restriction of freedom of speech in privacy cases, particularly in the context of disclosure of information.

95. In the UK, this is reflected in the requirement that, in privacy cases, the *European Convention on Human Rights* right to privacy (art 8) be balanced with the right to freedom of expression (art 10) when determining whether there has been an actionable invasion of privacy.[108] Additionally, s 12 of the *Human Rights Act 1998* (UK) makes special provision for considering the impact on freedom of expression in the grant of injunctions to restrain publication:[109]

> **s 12 Freedom of expression**
>
> (1) This section applies if a court is considering whether to grant any relief which, if granted, might affect the exercise of the Convention right to freedom of expression.
>
> …
>
> (4) The court must have particular regard to the importance of the Convention right to freedom of expression and, where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic material (or to conduct connected with such material), to—
>
> (a) the extent to which—
>
> (i) the material has, or is about to, become available to the public; or
>
> (ii) it is, or would be, in the public interest for the material to be published;
>
> (b) any relevant privacy code.

96. The ALRC is interested in submissions on whether a similar provision would be desirable in Australian legislation enacting a statutory cause of action or relating to other existing causes of action.

---

105 In *Bonnard v Perryman*, Lord Coleridge CJ stated that defamation cases require 'exceptional caution in exercising the jurisdiction to interfere by injunction before the trial of an action to prevent an anticipated wrong': *Bonnard v Perryman* [1891] 2 Ch 269, 283–85.

106 (2006) 227 CLR 57, [19].

107 In the past, many claimants in Australia used the action for defamation to protect their privacy against disclosure of embarrassing private facts, because in some states, the defendant could not defend the defamation merely on the basis that the imputations were true, but also had to show a public interest or public benefit in their publication. This is no longer the case due to changes to the law by the uniform state *Defamation Acts* of 2005: Carolyn Sappideen and Prue Vines (eds), *Fleming's Law of Torts* (Lawbook Co, 10th ed, 2011) 635–639.

108 *Campbell v MGN Ltd* [2004] 2 AC 457.

109 See Joint Committee on Privacy and Injunctions, *Privacy and Injunctions*, House of Lords Paper No 273, House of Commons Paper No 1443, Session 2010–12 (2012) 19–22.

**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)?

## Other remedies

97. As an alternative (or in addition) to monetary remedies and injunctions, there may be other remedies that are more appropriate where the statutory cause of action is made out.

98. The following remedies may be appropriate:

- an order requiring the defendant to apologise to the plaintiff;
- a correction order;
- an order for the delivery up, destruction or removal of material;
- a declaration; and
- an order that the defendant rectify its business or information technology practices.[110]

99. Each of these remedies may be appropriate in different circumstances. For some plaintiffs, all that will be sought is a formal acknowledgement that their privacy has been seriously invaded. For others, a serious invasion of privacy may have resulted in false information being published, which should be corrected. Where documents or other information have been published about the individual whose privacy has been seriously invaded, it may be appropriate to order that the documents or information be delivered to the individual, destroyed, or taken down from the internet. A declaration as to entitlements or the lawfulness or unlawfulness of certain conduct may be appropriate in some cases.

100. Serious invasions of privacy may also arise due to systemic problems with business processes or information technology systems, for instance, when a large company has inadequate controls to prevent staff from accessing customers' personal information without authorisation. Whether or not a systemic practice or failure amounts to an invasion of privacy for the purposes of a statutory cause of action would depend on the detailed design of the cause of action. If it did give rise to a cause of

110 Some of these remedies were recommended in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–5. The NSWLRC made similar recommendations, but noted that an order for destruction of material may not be appropriate where the plaintiff did not have property in the material: NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 57–69. The VLRC recommended that declarations be available in its report into surveillance in public places: Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Rec 29.

action, an appropriate remedy might be an order that the defendant rectify its business or information technology practices. It may however be more appropriate for such systemic breaches to be addressed by regulatory schemes where compliance can be monitored.

**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

### *Natural persons*

101. There appears to be significant agreement that a cause of action for invasion of privacy should only be able to be brought by, or in respect of, natural persons. Such a limitation has been considered appropriate because of the nature of the interest that a privacy cause of action is intended to protect. According to Sedley LJ, the protection of privacy is 'a legal principle drawn from the fundamental value of personal autonomy'.[111]

102. In *ABC v Lenah Game Meats*, Gummow and Hayne JJ observed that artificial persons could not invoke any such fundamental value to justify legal protection of their privacy. They noted that, 'of necessity, this artificial legal person lacks the sensibilities, offence and injury to which provide a staple value for any developing law of privacy'.[112]

103. In 2008, the ALRC recommended that a statutory cause of action for serious invasion of privacy should be limited to natural persons, 'on the basis that the desire to protect privacy is founded on notions of individual autonomy, dignity and freedom'.[113] Restriction to natural persons was uncontested in submissions to the DPM&C Issues Paper.[114]

104. Given that the restriction to natural persons appears to be uncontentious, the ALRC does not ask a question about this issue.

### *Deceased persons*

105. The ALRC considers here the question of whether, if a serious invasion of an individual's privacy occurs while that individual is alive, a cause of action should survive for the benefit of the estate.

---

111 *Douglas v Northern And Shell Plc* (2000) 2 WLR 992, [126].

112 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [126].

113 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2578.

114 See, eg, Australian Direct Marketing Association, Submission No 57 to DPM&C Issues Paper, 2011; Australian Privacy Foundation, Submission No 7 to DPM&C Issues Paper, 2011; Office of the Australian Information Commissioner, Submission No 14 to DPM&C Issues Paper, 2011; SBS, Submission No 8 to DPM&C Issues Paper, 2011.

106. This issue has been considered in previous law reform inquiries into privacy. The VLRC and NSWLRC recommended that a cause of action be restricted to living persons, with no action surviving for the benefit of an estate of an individual and no cause of action in respect of deceased persons whose privacy is invaded after their death.[115]

107. The ALRC does not consider at this stage of the Inquiry what further provisions the law should make about privacy-related matters in respect of deceased persons, such as about control of, access to or disclosure of information about deceased persons or their communications, or about physical interferences with the body or remains of a deceased person. The ALRC is interested however in receiving submissions that comment on particular problems that arise in the digital era with regard to control of or access, after death, to the private information or communications of individuals.

108. Traditionally at common law the rule *actio personalis moritur cum persona* meant that personal actions 'died' with the plaintiff so that no cause of action survived the plaintiff and that the estate of the plaintiff or victim could not sue with respect to wrongs suffered before death.[116] This position has been reversed in state and territory statutes so that some causes of action survive the death of the plaintiff, although the damages that may be awarded are limited after death in significant respects.[117] The limitation period for a survival action for serious invasion of privacy would be the same as the limitation period for the existing cause of action pursued during the plaintiff's lifetime. This position is consistent with limitation periods for negligence, nuisance and breach of duty survival claims in state Acts.[118]

109. However, an action analogous to a cause of action for invasion of privacy, the action for defamation, generally does not survive for the benefit of the defamed person's estate.[119] The rationale for this restriction is that a reputation is personal. Family members may only sue in defamation if they have been personally defamed.[120]

110. 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. This position would be consistent with existing survival legislation in relation to actions such as trespass to the person. However, if it were subject to existing restrictions—which generally prevent the estate recovering damages for non-pecuniary losses—there may be little point in the estate bringing the action (unless exemplary damages were

---

115 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Rec 32; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 71–72.

116 *Hambly v Trott* (1776) 1 Cowp 371; 98 ER 1136.

117 *Law Reform (Miscellaneous Provisions) Act 1944* (NSW); *Succession Act 1981* (Qld); *Survival of Causes of Action Act 1940* (SA); *Administration and Probate Act 1935* (Tas), *Administration and Probate Act 1958* (Vic); *Law Reform (Miscellaneous Provisions) Act 1941* (WA); *Civil Law (Wrongs) Act 2002* (ACT); *Law Reform (Miscellaneous Provisions) Act 1956* (NT).

118 For example, in NSW s 59(2) of the *Limitation Act 1969* (NSW) establishes the continuation of the pre-existing limitation period with the opportunity of a court extending the period by one year after the expiration of that limitation period.

119 See, eg, *Defamation Act 2005* (Qld) s 10. Compare *Administration and Probate Act 1935* (Tas) s 27.

120 *Krahe v TCN Channel Nine Pty Ltd* (1986) 4 NSWLR 536, 541.

available). It would be advisable for the legislation to specify what damages were available. In addition, a short limitation period in respect of the person's cause of action would limit the availability of a survival 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?

### *Proceedings in respect of other persons*

111. It may also be appropriate to allow an independent regulator, such as the Australian Privacy Commissioner, to bring proceedings on behalf of living, natural persons.[121] This approach may better enable access to justice for those with limited means, or in cases where systematic breaches of privacy affect a large number of individuals.[122]

112. The ALRC is interested in stakeholder response to such a proposal. It also seeks stakeholder views about who the most appropriate person or body would be to bring an action in respect of the serious invasion of privacy of one or more individuals.

113. Depending on which court or courts have jurisdiction, it is also possible that representative proceedings may be brought for serious invasion of privacy. For example, Part IVA of the *Federal Court of Australia Act 1976* (Cth) makes provision for representative proceedings, where the claims of several individuals can be combined and heard as a single proceeding.

> **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?

## Limitation period

114. Two important issues arise for the limitation period for a statutory cause of action for serious invasion of privacy: the length of any period; and the date from which the limitation period starts to run.

115. Should the limitation period be consistent with that of similar or related causes of action? For example, in defamation, the limitation period is one year, with a possible extension to three years if it was not reasonable in the circumstances to have

---

121 Law Institute of Victoria, Submission No 67 to DPM&C Issues Paper, 2011; Law Council of Australia, Submission No 55 to DPM&C Issues Paper, 2011; Maurice Blackburn Lawyers, Submission No 45 to DPM&C Issues Paper, 2011.

122 Law Institute of Victoria, Submission No 67 to DPM&C Issues Paper, 2011; Law Council of Australia, Submission No 55 to DPM&C Issues Paper, 2011.

commenced proceedings within one year.[123] For personal injury, the limitation period is three years.[124]

116. It may also be appropriate to start the limitation period from the date upon which the plaintiff became aware of the act or conduct constituting the invasion, rather than the date upon which the act or conduct occurred. The NSWLRC rejected the former approach, arguing that it was inconsistent with the general approach in Australia to the law of limitations.[125]

117. If the limitation period runs from the date the plaintiff first became aware of the invasion, the ALRC seeks stakeholder comment on whether there should be a maximum limitation period beyond which a cause of action could not be brought.

**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?

## Location and forum

118. The appropriate forums to hear a claim based on the statutory cause of action will depend on where the action is located—in Commonwealth, or in state and territory legislation.

119. The Terms of Reference require the ALRC to make recommendations concerning jurisdiction and access to justice. When considering these issues, a range of matters will need to be addressed including: minimising confusion or inconsistency in the application of legislation across Australian jurisdictions; the scope of available remedies; and any relevant constitutional issues.

### *Inclusion of a statutory cause of action in Commonwealth legislation*

120. The ALRC has previously recommended that a statutory cause of action be contained in Commonwealth legislation, separate to the *Privacy Act*, which would also cover state and territory agencies.[126] Depending on the specific design of a statutory cause of action, the constitutional power which the ALRC has previously identified as underpinning Commonwealth privacy legislation is the Australian Government's external affairs power.[127]

123 See, eg, *Limitation of Actions Act 1974* (Qld) ss 10AA, 32A. The NSWLRC recommended a similar limitation period: NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 70–71.

124 See, eg, *Limitation of Actions Act 1974* (Qld) s 11. The VLRC recommended a three-year limitation period: Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Rec 33.

125 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 71.

126 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–1, 2582.

127 *Australian Constitution* s 51(xxix); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 195–198.

121. Enshrining a statutory cause of action in Commonwealth legislation would grant jurisdiction to the Federal Court and Federal Circuit Court to hear actions. State courts may be empowered to hear federal matters by ss 71 and 77(ii) of the *Australian Constitution.*

122. The alternative approach, of having mirror legislation throughout the states and territories as well as in Commonwealth legislation, would depend for its efficacy on co-operation between the Commonwealth, states and territories to avoid inconsistency.

### *Inclusion in the Privacy Act*

123. Another approach is to place a statutory cause of action in the *Privacy Act*. This would require review of the scope of the Act and of the Australian Privacy Commissioner's powers. The Australian Privacy Commissioner's current remit is to investigate interferences with privacy which disclose personal information.[128] A statutory cause of action would probably involve a wider range of invasive conduct.

124. Currently, the Australian Privacy Commissioner may investigate complaints and make non-binding determinations.[129] Where a Commonwealth agency has not complied with a determination, the Commissioner or the complainant may pursue the matter in the Federal Court or Federal Circuit Court.[130] An individual who has lodged a complaint with the Privacy Commissioner may appeal a determination or a decision not to investigate a complaint through three alternate channels: the federal courts; the Administrative Appeals Tribunal (AAT); or the Commonwealth Ombudsman.

125. Other models include granting jurisdiction to state or Commonwealth administrative review tribunals. This may be in addition to the jurisdiction of the federal courts. These forums offer litigants relatively lower costs in legal representation and court costs, informality in proceedings and alternative dispute resolution paths. These factors may minimise the chance of high adverse costs orders which may result from court proceedings. This approach may be appealing to enable broader access to justice for claimants. Decisions from state-based administrative review tribunals may be appealed on questions of law to state supreme courts.

**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?

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

128 *Privacy Act 1988* (Cth) s 13.
129 Ibid ss 36, 40, 52.
130 Ibid s 55A.

### *Alternative dispute resolution*

126. While a statutory cause of action would provide individuals with a mechanism to seek redress for serious invasions of privacy in a court, judicial proceedings are likely to be expensive, with no guarantee of a favourable outcome. Alternative dispute resolution (ADR) can provide a faster, cheaper and low-risk alternative to judicial proceedings.

127. Common ADR options include mediation, conciliation and arbitration. In mediation, the parties to the dispute attempt to reconcile their disagreement themselves, with a neutral mediator present to assist the parties in reaching an agreement, but not to provide advice. In conciliation, a neutral third party provides advice, but does not make a determination. In arbitration, the parties present their arguments to a neutral arbitrator, who makes a determination. ADR services are usually provided by specialist mediators, conciliators and arbitrators.

128. Some court rules already require parties to attempt mediation in the early stages of proceedings or a court may have the power to direct parties to engage in a mediation process.[131]

129. While ADR has significant advantages, it may also have disadvantages. The most significant disadvantage is that the outcomes of ADR are generally not binding on the parties. As a result, there is potential for ADR to be misused by some parties as a delaying tactic, which may add to the final time and costs if the dispute proceeds to court. There may also be a public interest in having certain cases heard in court—for example, where it would be helpful to have a judicial ruling on certain conduct involving new technologies.[132]

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

## Interaction with existing complaints processes

130. The ALRC is interested in submissions on the overlap and interaction of a statutory cause of action with the existing regulatory and remedial regime governing information privacy.

131. A number of existing statutory bodies have the power to respond to complaints about certain categories of invasion of privacy. These include, for example:

- the Australian Privacy Commissioner;

131 See for example *Civil Procedure Act 2005* (NSW) pts 4, 5; *Civil Procedure Act 2010* (Vic) ch 5; *Federal Court of Australia Act 1976* (Cth) s 53A.

132 For discussions of the benefits and limitations of ADR, see, eg, Law Reform Commission of Ireland, *Alternative Dispute Resolution: Mediation and Conciliation*, Report LRC 98-2010 (2010) ch 1; 'Alternative Dispute Resolution: General Civil Cases' (New Zealand Ministry of Justice, 2004) ch 4.

- the privacy and information commissioners in each state and territory;
- other regulators, such as the Australian Communications and Media Authority (ACMA) and the Australian Competition and Consumer Commission (ACCC); and
- industry bodies such as the Australian Press Council and the Telecommunications Industry Ombudsman.

132. Some of these bodies (the privacy and information commissioners) have a particular focus on data protection. Others have more general functions, with privacy complaints being one among many types of complaints handled. The possible outcomes of the complaints processes also vary between these bodies, ranging from non-binding recommendations to enforceable determinations.

133. The Australian Privacy Commissioner, in particular, may have the power to handle many complaints that could also be the basis for a statutory cause of action—for example, complaints about improper use or disclosure of personal information. The Privacy Commissioner's powers extend to Australian Government and private sector organisations (with some specific exemptions).

134. In dealing with complaints under the *Privacy Act*, the Privacy Commissioner may make a range of determinations, from dismissing the complaint to a declaration that the complainant is entitled to monetary compensation for loss or damage suffered, or that the respondent must take specified steps to ensure that the conduct is not repeated or continued.[133]

135. It may be appropriate to limit judicial actions where a non-judicial process has been used to resolve a complaint. This would reduce the possibility of complainants 'double-dipping' to take advantage of multiple avenues of dispute resolution.

**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?

## Other legal remedies to prevent and redress serious invasions of privacy

136. The Terms of Reference require the ALRC to make recommendations as to legal remedies to redress serious invasions of privacy, other than a statutory cause of action, and also as to innovative ways in which the law might reduce serious invasions of

133 *Privacy Act 1988* (Cth) s 52. The Privacy Commissioner is also empowered to deal with complaints arising under other legislation with relevance to privacy, such as the *Healthcare Identifiers Act 2010* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth). Contravention of certain provisions in these Acts constitutes 'an interference with the privacy of an individual' under the *Privacy Act 1988* (Cth).

privacy. Both of these aspects of the Terms of Reference need to be considered against the background of existing laws. This section of the Issues Paper gives a very brief survey of existing laws. It also poses some preliminary questions about ways in which the law or regulatory frameworks could be reformed to more effectively prevent and redress serious invasions of privacy.

137. As set out above in the 'Scope of the Inquiry', the ALRC does not propose to revisit legislation that has only recently been introduced or amended in significant ways, after extensive deliberation and consultation. Submissions would be welcome, however, on aspects of Commonwealth legislation that have not been recently considered and that it may be appropriate to review in order to provide greater and more accessible protection of individual privacy.

138. With respect to relevant state and territory legislation, the ALRC is particularly interested in key ways in which legislative provisions diverge in the various jurisdictions on privacy matters, as uniformity of legislation across Australia is generally desirable. Uniform legislation tends to promote clarity, comprehensibility, ease of application and compliance, and efficiency. All of these in turn better promote the policies that underpin the legislation.

## The *Privacy Act 1988* (Cth)

139. The *Privacy Act* is Australia's key data protection law.[134] The *Privacy Act* provides 13 'Australian Privacy Principles' (APPs) that set out the broad requirements on collection, use, disclosure and other handling of personal information.[135] Personal information is defined in s 6(1) of the Act as information or opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not in material form.

140. The Act applies to 'APP entities'—Australian Government agencies and large private sector organisations with a turnover of more than $3 million. Certain small businesses are also covered, such as those that provide health services and those that disclose personal information to anyone else for a benefit, service or advantage.[136] The APPs cover many aspects of information privacy.

141. In addition to the APPs, the *Privacy Act* grants a range of powers to the Australian Privacy Commissioner, including:

- investigating complaints made by individuals or on the Commissioner's own motion about APP entities;[137]

---

134 The *Privacy Act 1988* (Cth) has been the subject of recent reforms following the ALRC's previous Privacy Inquiry. A number of recommendations made in ALRC Report 108 have been implemented in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). These amendments will come into effect from March 2014, and the discussion in this Issues Paper reflects the law as it will stand from that date.

135 *Privacy Act 1988* (Cth) sch 1.

136 The definition of 'APP entity' is given in s 6(1) of the *Privacy Act 1988* (Cth). Small businesses are not, in general, APP entities, with some exceptions as set out in s 6D of the Act.

137 *Privacy Act 1988* (Cth) pt V.

- directing agencies to conduct privacy impact assessments;[138] and
- applying for Federal Court and Federal Circuit Court orders for civil penalties for serious or repeated breaches of the APPs.[139]

142. A breach of an APP in respect of personal information is an 'interference with the privacy of an individual'. Serious or repeated contraventions may give rise to a civil penalty order.[140]

143. State and territory legislation creates data protection requirements similar to those under the *Privacy Act*, with application to state and territory government agencies, as well as (variously) local councils, government-owned corporations and universities.[141]

144. The existing Commonwealth, state and territory legislation applies to major organisations such as banks, large retailers, government departments and utilities providers, which collect and store personal information. There are a large number of organisations that are exempt from the application of all of these Acts and whose activities may have an impact on individual privacy. These may include, for example, many small businesses.[142]

## Health information privacy

145. Health and genetic information is recognised as sensitive information under the *Privacy Act*, a status which provides it with stronger protections under the APPs than those protections applying to personal information more generally.[143] Separate Commonwealth Acts protect healthcare identifiers[144] and electronic health records.[145]

146. Several state and territory laws also offer protections, including limitations on collection, use and disclosure, for health information held by state and territory public and private sector organisations.[146]

## Communications privacy

147. The *Telecommunications Act 1997* (Cth) (*Telecommunications Act*) provides a broad regulatory framework for telecommunications services, including internet services, with specific provisions prohibiting the disclosure, by telecommunications

---

138 Ibid s 33D.
139 Ibid s 80W.
140 Ibid s 13G.
141 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Premier and Cabinet Circular No 12* (SA); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic); *Information Act* (NT). The *Privacy Act 1988* (Cth) has application to agencies in the Australian Capital Territory.
142 *Privacy Act 1988* (Cth) s 6C.
143 The definition of 'sensitive information' is given in s 6(1) of the *Privacy Act 1988* (Cth). A number of the APPs make special provisions for sensitive information: see, eg, APP 3.
144 *Healthcare Identifiers Act 2010* (Cth).
145 *Personally Controlled Electronic Health Records Act 2012* (Cth).
146 *Health Records and Information Privacy Act 2002* (NSW); *Information Privacy Act 2009* (Qld); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act* (NT).

providers and several other types of organisation, of certain information.[147] Contravention of these prohibitions is an offence punishable by up to two years imprisonment.[148] A number of exemptions from the non-disclosure requirements of the *Telecommunications Act* exist under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), for example, for disclosures to ASIO or the Australian Federal Police.[149]

148. The TIA Act also creates offences for improperly intercepting communications.

## Surveillance laws

149. Under state and territory surveillance laws, it is illegal to record or store and distribute a recording of a private conversation obtained without the consent of the other party.[150] Under Part 2 of the *Surveillance Devices Act 1999* (Vic), the installation or use of various types of surveillance device is punishable by up to 240 penalty units or imprisonment for up to two years. However, each Act varies significantly in the devices and conduct prohibited.

150. The *Surveillances Devices Act 2004* (Cth) criminalises the use of listening devices, optical devices, tracking and data surveillance devices without the consent of the party who is being recorded.[151] This Act is restricted to the actions of Australian Government agencies and their employees.[152]

151. Different state and territory workplace surveillance legislation prohibits employers monitoring their employees at work through covert surveillance methods such as the use of CCTV cameras or computer, internet and email surveillance.[153]

## Criminal laws

### *Harassment and stalking offences*

152. State and territory laws criminalising harassment and stalking vary considerably depending on the jurisdiction. Legislation in Queensland and Victoria expressly prohibits 'cyber-harassment' committed through 'electronic messages'[154] or by

147 *Telecommunications Act 1997* (Cth) pt 13.
148 Ibid s 276.
149 Section 180F of the TIA Act requires that, before disclosure of information is made under div 4 or 4A, an authorised officer 'must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable'.
150 *Surveillance Devices Act 2007* (NSW); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act* (NT).
151 *Surveillance Devices Act 2004* (Cth) ss 7–10.
152 Ibid s 3.
153 *Workplace Surveillance Act 2005* (NSW); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic); *Surveillance Devices Act 1998* (WA); *Workplace Privacy Act 2011* (ACT).
154 *Crimes Act 1958* (Vic) s 21A(2)(b).

'otherwise contacting the victim'.[155] There is no Commonwealth legal framework to protect the 'cyber-safety' of minors, which may overlap with privacy concerns.[156]

### *Criminal sanctions against indecent photography*

153. Criminal sanctions apply where photography is used for indecent purposes.[157] South Australia, Queensland, Victoria, Tasmania and NSW have enacted specific provisions in criminal law to prohibit indecent filming without consent.[158] However other states do not have similar provisions.

154. The criminal law provides protection against indecent photography of children in private and public places.[159]

### *Other criminal sanctions*

155. Criminal sanctions currently exist for some specific invasions of privacy. For example, under s 62 of the *Privacy and Personal Information Protection Act 1998* (NSW) the unauthorised or corrupt use or disclosure by a public official of personal information obtained through their official functions is an offence punishable by up to 100 penalty units or imprisonment for up two years.

## Industry codes and guidelines

156. Various statutory and self-regulatory bodies oversee and enforce industry codes and guidelines which protect against invasions of privacy. The enforcement capabilities of these bodies vary significantly.

157. The ACMA is empowered under the *Broadcasting Services Act 1992* (Cth) to regulate the *Commercial Radio Australia Codes of Practice and Guidelines* (2011), the *Internet Industry Code of Practice* (2008) and the *Commercial Television Industry Code of Practice* and the *Privacy Guidelines for Broadcasters* (2010).[160] The ACMA is empowered to investigate and issue take-down notices of online content.[161] However this latter system is primarily concerned with regulating offensive content or prohibited content under the *National Classification Code*, rather than the protection of an individual's privacy.

158. The Australian Press Council oversees the adherence of its members to its *Charter of Press Freedom* (2003) and *Statement of Privacy Principles* (2011).

---

155 *Criminal Code Act 1899* (Qld) s 359A(7)(b).

156 Other jurisdictions have enacted national legislative frameworks to safeguard the cyber-safety of children—for example, Nova Scotia's *Cyber-safety Act* SNS 2013, c 2. Similarly, the US federal government has enacted the *Children's Online Privacy Protection Act*, 15 USC §§ 6501-6506 (1998).

157 *Summary Offences Act 1988* (NSW) s 4; *Criminal Code Act 1899* (Qld) s 227(1); *Police Offences Act 1935* (Tas) s 13.

158 *Crimes Act 1900* (NSW) ss 91K–91M; *Criminal Code Act 1899* (Qld) s 227A(1); *Summary Offences Act 1953* (SA) s 26D; *Police Offences Act 1935* (Tas) s 13A; *Summary Offences (Upskirting) Act 2007* (Vic) s 41A.

159 See, eg, *Criminal Law Consolidation Act 1935* (SA) s 63B.

160 *Broadcasting Services Act 1992* (Cth) pt 9B.

161 *Broadcasting Services Act 1992* (Cth) sch 7.

159. Part IIIB of the *Privacy Act* makes provision for the development of privacy codes (APP codes). APP codes can be developed on the initiative of 'code developers', or in response to a request from the Privacy Commissioner. The Commissioner may also develop an APP code. The codes set out compliance requirements for one or more APPs. The code developer may apply to the Commissioner to have the code registered. A breach of a registered code constitutes an 'interference with privacy' under the Act, and if the breach is serious or repeated the Commissioner may apply to the Federal Court or Federal Circuit Court for a civil penalty order.

## Common law causes of action

160. There are a number of causes of action at common law which can, in some cases, be used to protect privacy or have the effect of protecting personal privacy.[162] These causes of action protect against physical intrusions upon, and surveillance of, a person and against unauthorised disclosure of private information.

161. They include:

- the tort actions for trespass to the person, particularly battery and assault;
- the tort of trespass to land,[163] including interferences with airspace not protected by legislation;[164]
- the tort of nuisance,[165] including interferences with airspace not protected by legislation;
- the tort of defamation;[166] and
- the equitable action for breach of confidence.[167]

## Gaps in existing law

162. Although the existing law provides significant protection against some invasions of privacy, there are significant gaps or uncertainties in the protection that existing legislation and common law actions provide for serious invasions of privacy. These include the following:

---

162 Carolyn Sappideen and Prue Vines (eds), *Fleming's Law of Torts* (Lawbook Co, 10th ed, 2011) ch 26.

163 Trespass to land is often used to protect privacy. See, eg, *TCN Channel Nine Pty Ltd v Anning* (2002) 54 NSWLR 333; *TCN Channel Nine Pty Ltd v Ilvariy Pty Ltd* (2008) 71 NSWLR 323.

164 For example, the *Civil Liability Act 2002* (NSW) s 72 provides limited protection against a trespass or nuisance action for a flight in airspace at a reasonable height and in compliance with air navigation regulations.

165 *Raciti v Hughes* (1995) 7 BPR 14,837.

166 Carolyn Sappideen and Prue Vines (eds), *Fleming's Law of Torts* (Lawbook Co, 10th ed, 2011) ch 25.

167 This action has been the basis of the enhanced common law protection of privacy in the United Kingdom since the *Human Rights Act 1998* (UK). In *Campbell v MGN Ltd* [2004] 2 AC 457, the action for breach of confidence developed into an action against the disclosure and misuse of personal information. This was accepted in *ABC v Lenah Game Meats*, so that the obligation of confidence arises on the receipt of confidential or private information, removing the need for a pre-existing relationship of confidence: (2001) 208 CLR 199, 224.

- The *Privacy Act* and state and territory equivalents deal only with information privacy and not with intrusions into personal privacy.
- The *Privacy Act* provides for only limited civil redress to individuals who are affected by a breach of the APPs.
- There are a number of organisations that are exempt from the application of the regulatory regime of existing privacy legislation, such as many businesses with an annual turnover of less than $3 million.
- Legislation dealing with surveillance in general, and with workplace surveillance, is not uniform throughout Australia.
- There is no tort or civil action for harassment, nor is there sufficient deterrence against 'cyber-harassment' in Australian law, compared with overseas jurisdictions.[168]
- The tort actions of trespass to the person, trespass to land and nuisance do not provide protection from intrusion into a person's private activities in many situations.[169]
- Legislation and common law protection against aerial and other surveillance does not reflect advances in technology that provide a capacity for new types of invasion into personal privacy.[170]
- Tort law does not provide a remedy for intentional infliction of emotional distress which does not amount to psychiatric illness.[171]
- While the equitable action for breach of confidence can provide effective legal protection against the disclosure of private information, it is less effective after a wrongful disclosure because it is unclear or uncertain whether a plaintiff may recover compensation for emotional distress.[172]
- There is uncertainty, or at least some debate, as to the relevant principles to be applied when a court is considering whether to grant an injunction to restrain the publication of true, private information.[173]

---

168 A number of US states have enacted cyber-stalking or cyber-harassment legislation or have laws that explicitly include electronic forms of communication within more traditional stalking or harassment laws. Most of these constitute amendments to State Criminal Codes, updating the meaning of harassment and/or stalking to include electronic communications. In Nova Scotia in Canada, the *Cyber-safety Act*, SNS 2013, c 2 criminalises cyber-bullying.

169 Trespass to the person requires bodily contact or a threat of such contract to be actionable. Both trespass to land and nuisance protect only the occupier of the relevant land, and the former requires an intrusion onto the land.

170 An example is the increasing use of drones to carry out unauthorised aerial surveillance.

171 *Wainwright v Home Office* [2004] AC 406; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.

172 See *Giller v Procopets* (2008) 24 VR 1.

173 The guidance provided by defamation cases is debatable given the differences between privacy and defamation actions: see *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57. See also David Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy' (2012) 17 *Media and Arts Law Review* 170; Godwin Busuttil and Patrick McCafferty, 'Interim Injunctions and the Overlap Between Privacy and Libel' (2010) 2 *Journal of Media Law* 1.

- There is no clear legislative statement protecting freedom of speech, or explicitly requiring it or other matters of public interests to be balanced with the protection of privacy, when the court is considering the grant of an injunction to restrain publication of information or some other alleged invasion of privacy.[174]

163. The ALRC is interested in receiving submissions about significant ways in which existing regulatory frameworks or legal remedies may be amended or strengthened to better 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?

**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?

## Innovative ways to reduce serious invasions of privacy in the digital era

164. New and emerging technologies in the digital era challenge the effectiveness of protection for privacy provided by existing legal principles and regulatory frameworks:

- Highly portable and increasingly affordable consumer devices, such as smartphones, are capable of holding substantial amounts of private information, including photographs, video and audio content. This information can be instantly uploaded to the internet and shared with a wide audience.
- Consumers and businesses are increasingly making use of third-party services (eg 'cloud' services) to store data, putting the information further away from the direct control of the individual or business.
- Information about individuals—including their physical and online shopping activity, location and use of social networks—can be gathered almost continuously. New methods of sharing, analysing or aggregating this information (often described as 'big data') have emerged that form the basis of new internet business models.

174 See the discussion at paragraph 95, above, on principles set out in the *Human Rights Act 1998* (UK) s 12 relevant to the granting of injunctions in privacy cases.

- Social media platforms have expanded so that social media content can be shared by a relatively large number of people in a relatively short time.
- Individuals are often unaware of the scope of information collected about them without their knowledge. Further, despite formally accepting the terms and conditions imposed by the provider of an online service or app, individuals are often unaware of particular uses that may be made of information they have voluntarily or unwittingly provided.

165. There are a number of ways in which the law might respond to these new situations. The ALRC sets out below some preliminary observations and then seeks submissions on options which would be suitable for consideration in this Inquiry.

### *Reviewing the role of consent in consumer contracts in the digital era*

166. Australia's existing data protection laws can be characterised as using a 'consent-based' model. The APPs and other restrictions on the handling of personal information typically contain exemptions when an individual has given consent for his or her personal information to be collected, used, or disclosed. Many of the privacy protections in other Commonwealth, state and territory laws operate on a similar model, and the model forms the basis of a large proportion of the data protection and privacy laws globally.[175]

167. The fact that an individual engages with a commercial provider of internet services or applications after accepting various terms and conditions brings into play both the common law of contract and the statutory regimes for consumer protection such as the Australian Consumer Law (ACL).[176] For example, the terms and conditions may be unclear or ambiguous, or may not cover the use of the information that is at issue. In some cases, a provider might be held to have engaged in misleading or deceptive conduct in breach of the ACL.[177]

168. Recent commentary has suggested that the consent-based model of data protection cannot adequately respond to emerging methods of data collection and use.[178]

---

175 Notably, the OECD's privacy guidelines, on which many data protection laws are based, allow collection or use of personal information with the consent of the individual: see Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013.

176 *Competition and Consumer Act 2010* (Cth) sch 2.

177 The prohibition on misleading or deceptive conduct in s 18 of the ACL applies where the party is engaged in trade or commerce. Many providers would be acting in trade or commerce regardless of whether or not they charge the consumer for the particular service: see the definition of 'trade or commerce' in sch 2 par 2 of the *Competition and Consumer Act 2010* (Cth).

178 Daniel J Solove, 'Privacy Self-management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.

### *Providing individuals with an enforceable right to removal of certain information*

169. Social media services allow individual users to connect and share information with each other. The ease of sharing enabled by these services means that control over this information may be lost. Further, information may continue to be available indefinitely.

170. One possible solution to the loss of control over information, recently proposed in Europe, is the introduction of a 'right to be forgotten and to erasure'. This proposal would introduce a requirement that organisations, such as social media service providers, permanently delete information at the request of the individual who is the subject of that information.[179]

171. In the Australian context, some protection against ongoing exposure of private information may be available if data controllers (such as APP entities) were required, in limited circumstances, to delete an individual's personal information on request.

### *Dealing with tracking technology*

172. Various tracking technologies allow the websites visited by an individual to be reported to websites or services visited by that individual. Tracking of online activity appears to be an area of concern for many individuals.[180]

173. Online tracking systems can be used to provide outcomes that many people desire, such as customised advertising. However, many people may want more control over whether they are subject to tracking. Globally, there has been growing interest in 'Do Not Track' (DNT) requests. DNT allows a user to request that websites not use online tracking tools like those described above. DNT requests are available in most modern web browsers, but there is no requirement that a website operator or service provider honour DNT requests.[181]

174. Offline tracking is enabled by a range of systems, such as devices using Global Positioning System (GPS) receivers that allow a mobile device to record its locations over time and to report those locations. There is a public interest in much of this data, for example, for emergency services or for monitoring network traffic. However, offline tracking and the use of location data more generally may also raise privacy issues. The location of an individual at certain times can reveal, for instance, the

---

179 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)', art 17. The right to be forgotten would be subject to limitations protecting, among other things, freedom of expression and the public interest in public health.

180 'Privacy and Personal Data' (Occasional Paper No 4, Australian Communications and Media Authority, June 2013).

181 The development of a DNT standard appears to have been slowed by disagreement among the parties involved about the specific activities a website could continue to conduct while honouring a DNT request: see Natasha Singer and Somini Sengupta, '"Do Not Track" Rules Come a Step Closer to an Agreement' *New York Times*, 15 July 2013 <www.nytimes.com/2013/07/16/technology/do-not-track-rules-for-advertising-to-web-users-come-a-step-closer-to-an-agreement.html>.

individual's religious views, political affiliations, medical conditions or private activities.

175. A 2012 report by the ACMA found that the risks of location data were poorly understood by consumers. Further, consumers expected to be provided with better information about how location data is used and to be able to make informed choices about whether or not to allow their location data to be used.[182] Online and offline tracking may be better regulated within existing consumer and information privacy frameworks.

### *Broadening the regulation of use of metadata*

176. There has been increasing concern expressed about the use of metadata. Metadata about a communication includes the time, origin, destination and duration of a communication, rather than the content. Metadata is often excluded from the privacy protection that applies to other data. For example, ss 276–278 of the *Telecommunications Act* prohibit only the disclosure of 'the contents or substance of a communication'. However, metadata can also be analysed to reveal private information about the communication and an individual.[183] It may be appropriate for some existing prohibitions about unauthorised data disclosure to be reviewed.

### *Dealing with aggregation of data*

177. One characteristic of the digital era is the widespread collection of seemingly insignificant data into large data sets. This data can include, for instance, information uploaded by individuals to social media services, online or offline purchase history, information about individuals' social networks (eg, the 'friends' of individuals), location data, and web browsing history. Aggregation of this data can often reveal unexpected personal or sensitive information about individuals.[184]

178. A related problem is the use of large datasets to re-identify information that is initially thought to be anonymous, or de-identified. In April 2013, the Office of the Australian Information Commissioner released for consultation draft guidelines on de-identification of personal information, noting that future technologies and future increases in available data may change the risk of re-identification.[185]

### *Prohibiting employer requests for access to private social media accounts*

179. An area of growing concern is the use of social media to assess candidates for work, education and other opportunities.

---

182 'Here, There and Everywhere: Consumer Behaviour and Location Services' (Australian Communications and Media Authority, December 2012).

183 'A Primer on Metadata: Separating Fact from Fiction' (Information and Privacy Commissioner, Ontario, July 2013).

184 Michal Kosinski, David Stillwell and Thore Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) 110 *Proceedings of the National Academy of Sciences* 5802.

185 Office of the Australian Information Commissioner, *De-identification Resources May 2013* <www.oaic.gov.au>.

180. A threat to privacy comes from an employer or other individual making unconscionable use of his or her position of advantage or power by requesting or demanding access to an individual's private social media accounts. Such requests have been prohibited in various jurisdictions, in particular in a number of US states.[186] It is unclear whether the practice of requiring social media passwords or other similar information is widespread in Australia. It may be appropriate to include such conduct as an example of a serious invasion of privacy for the purpose of a statutory cause of action or to amend laws dealing with workplace surveillance to prohibit such conduct.

### *Regulating aerial surveillance*

181. Existing laws with regard to incursions into airspace tend to have been drafted at a time when surveillance technologies were less developed. Compliance with air navigation rules drafted for the purpose of ensuring safety and for protecting commercial and private flights from liability for mere passage through private airspace may not properly address privacy concerns about deliberate aerial surveillance or data recording by the media and others.[187]

182. Further, in Australia, there has recently been an increase in the use by civilians of remotely piloted aircraft (RPAs), commonly known as drones. While some use of RPAs appears to be merely recreational, there have been increasing reports of the use of RPAs to carry out targeted surveillance of the activities of other individuals, businesses or organisations.[188] This may raise privacy concerns that existing air navigation laws and regulations do not address.

183. It may be appropriate to consider how existing laws and regulations could better prevent or redress serious invasion of privacy by deliberate aerial surveillance activities, including the use of RPAs.

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

186 For example, in New Jersey: PL 2013 c 55.

187 For example, *Civil Liability Act* 2002 (NSW) s 72 grants an exemption from liability in trespass or nuisance.

188 See, eg, Renee Viellaris, 'Unmanned Aircraft Bought Online Being Deployed to Monitor Private and Public Property' *Courier Mail*, 31 August 2013.