Australian Government
Australian Law Reform Commission

Serious Invasions of Privacy in the Digital Era

DISCUSSION PAPER

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

Discussion Paper 80 (DP 80) March 2014

This Discusion Paper reflects the law as at 31st March 2014

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: 978-0-9873872-9-5

Commission Reference: ALRC Discussion Paper 80, 2014

Making a submission

Any public contribution to an inquiry is called a submission. The Australian Law Reform Commission (ALRC) 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 Discussion Paper is 12 May 2014.

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/privacy-subs-DP80. 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.

The ALRC may redact certain information from submissions in order to protect the privacy of submitters or others mentioned in submissions. This may include withholding the name of the submitter. Publication or redaction of information in submissions is at the discretion of the ALRC.

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

Participants

Australian Law Reform Commission

President

Professor Rosalind Croucher

Commissioner in Charge

Professor Barbara McDonald

Part-time Commissioners

The Hon Justice John Middleton

Executive Director

Sabina Wynn

Senior Legal Officers

Jared Boorer

Legal Officers

Brigit Morris

Steven Robertson

Legal Interns

Claire Bready

Ravi Gosal

Michelle Meares

Jack Murray

Hagen Sporleder

Jackson Wherrett

Bradley Woods

Advisory Committee Members

The Hon Justice Peter D Applegarth, Queensland Supreme Court

Richard Coleman, Fairfax Media Limited

Professor Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales

Anna Johnston, Director, Salinger Privacy

Peter Leonard, Partner, Gilbert & Tobin

The Honourable W H Nicholas

Tara McNeilly, Senior General Counsel, OGC, Australian Government Solicitor

Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner

Professor Megan Richardson, Melbourne Law School, University of Melbourne

Associate Professor David Rolph, Sydney Law School, University of Sydney

Edward Santow, Chief Executive Officer, Public Interest Advocacy Centre

Veronica Scott, Special Counsel, Media and Communications Group, Minter Ellison

David Vaile, Executive Director, Cyberspace Law and Policy Centre, UNSW Faculty of Law

Proposals and Questions

4. A New Tort in a New Commonwealth Act

Proposal 4–1 A statutory cause of action for serious invasion of privacy should be contained in a new Commonwealth Act (the new Act).

Proposal 4–2 The cause of action should be described in the new Act as an action in tort.

5. Two Types of Invasion and Fault

Proposal 5–1 **First element of action:** The new tort should be confined to invasions of privacy by:

(a) intrusion upon the plaintiff's seclusion or private affairs (including by unlawful surveillance); or

(b) misuse or disclosure of private information about the plaintiff (whether true or not).

Proposal 5–2 **Second element of action:** The new tort should be confined to intentional or reckless invasions of privacy. It should not extend to negligent invasions of privacy, and should not attract strict liability.

Proposal 5–3 The new Act should provide that an apology made by or on behalf of a person in connection with any invasion of privacy alleged to have been committed by the person:

(a) does not constitute an express or implied admission of fault or liability by the person in connection with that matter; and

(b) is not relevant to the determination of fault or liability in connection with that matter.

Proposal 5–4 Evidence of an apology made by or on behalf of a person in connection with any conduct by the person is not admissible in any civil proceedings as evidence of the fault or liability of the person in connection with that matter.

6. A Reasonable Expectation of Privacy

Proposal 6–1 **Third element of action:** The new tort should only be actionable where a person in the position of the plaintiff would have had a reasonable expectation of privacy, in all of the circumstances.

Proposal 6–2 The new Act should provide that, in determining whether a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances, the court may consider, among other things:

(a) the nature of the private information, including whether it relates to intimate or family matters, health or medical matters, or financial matters;

(b) the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology;

(c) the place where the intrusion occurred;

(d) the purpose of the misuse, disclosure or intrusion;

(e) how the private information was held or communicated, such as in private correspondence or a personal diary;

(f) whether and to what extent the private information was already in the public domain;

(g) the relevant attributes of the plaintiff, including the plaintiff's age and occupation;

(h) whether the plaintiff consented to the conduct of the defendant; and

(i) the extent to which the plaintiff had manifested a desire not to have his or her privacy invaded

7. Seriousness and Proof of Damage

Proposal 7–1 **Fourth element of action:** The new Act should provide that the new cause of action is only available where the court considers that the invasion of privacy was 'serious'. The new Act should also provide that in determining whether the invasion of privacy was serious, a court may consider, among other things, whether the invasion of privacy was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff.

Proposal 7–2 The plaintiff should not be required to prove actual damage to have an action under the new tort.

8. Balancing Privacy with Other Interests

Proposal 8–1 **Fifth element of action:** The new Act should provide that the plaintiff only has a cause of action for serious invasion of privacy where the court is satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest. A separate public interest defence would therefore not be needed.

Proposal 8–2 The new Act should include the following non-exhaustive list of public interest matters which a court may consider:

(a) freedom of expression, including political communication;

(b) freedom of the media to investigate, and inform and comment on matters of public concern and importance;

(c) the proper administration of government;

(d) open justice;

(e) public health and safety;

(f) national security;

(g) the prevention and detection of crime and fraud; and

(h) the economic wellbeing of the country.

9. Forums, Limitations and Other Matters

Proposal 9–1 Federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy under the new Act.

Question 9–1 If state and territory tribunals should also have jurisdiction, which tribunals would be appropriate and why?

Proposal 9–2 The new Act should provide that the new tort be limited to natural persons.

Proposal 9–3 A cause of action for serious invasion of privacy should not survive for the benefit of the plaintiff's estate or against the defendant's estate.

Proposal 9–4 A person should not be able to bring an action under the new tort after either (a) one year from the date on which the plaintiff became aware of the invasion of privacy, or (b) three years from the date on which the invasion of privacy occurred, whichever comes earlier. In exceptional circumstances the court may extend the limitation period for an appropriate period, expiring no later than three years from the date when the invasion occurred.

Proposal 9–5 The new Act should provide that, in determining any remedy, the court may take into account:

(a) whether or not a party took reasonable steps to resolve the dispute without litigation; and

(b) the outcome of any alternative dispute resolution process.

10. Defences and Exemptions

Proposal 10–1 The new Act should provide a defence of lawful authority.

Proposal 10–2 The new Act should provide a defence for conduct incidental to the exercise of a lawful right of defence of persons or property where that conduct was proportionate, necessary and reasonable.

Proposal 10–3 The new Act should provide for a defence of absolute privilege for publication of private information that is co-extensive with the defence of absolute privilege to defamation.

Proposal 10–4 The new Act should provide for a defence of qualified privilege to the publication of private information where the defendant published matter to a person (the recipient) in circumstances where:

(a) the defendant had an interest or duty (whether legal, social or moral) to provide information on a subject to the recipient; and

(b) the recipient had a corresponding interest or duty in having information on that subject; and

(c) the matter was published to the recipient in the course of giving to the recipient information on that subject.

The defence of qualified privilege should be defeated if the plaintiff proves that the conduct of the defendant was actuated by malice.

Question 10–1 Should the new Act instead provide that the defence of qualified privilege is co-extensive to the defence of qualified privilege to defamation at common law?

Proposal 10–5 The new Act should provide for a defence of publication of public documents.

Proposal 10–6 The new Act should provide for a defence of fair report of proceedings of public concern.

Question 10–2 Should the new Act provide for a defence of necessity?

Proposal 10–7 The new Act should provide a safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their service.

Question 10–3 What conditions should internet intermediaries be required to meet in order to rely on this safe harbour scheme?

11. Remedies and Costs

Proposal 11–1 The new Act should provide that courts may award compensatory damages, including damages for the plaintiff's emotional distress, in an action for serious invasion of privacy.

Proposal 11–2 The new Act should set out the following non-exhaustive list of factors that may mitigate damages for serious invasion of privacy:

(a) that the defendant has made an appropriate apology to the plaintiff about the conduct that invaded the plaintiff's privacy;

(b) that the defendant has published a correction of any untrue information disclosed about the plaintiff;

(c) that the defendant has made an offer of amends in relation to the defendant's conduct or the harm suffered by the plaintiff;

(d) that the plaintiff has already recovered compensation, or has agreed to receive compensation in relation to the conduct of the defendant;

(e) that the defendant had taken reasonable steps to settle the dispute with the plaintiff in order to avoid the need for litigation; and

(f) that the plaintiff had not taken reasonable steps to settle the dispute, prior to commencing or continuing proceedings, with the defendant in order to avoid the need for litigation.

Proposal 11–3 The new Act should set out the following non-exhaustive list of factors that may aggravate damages for serious invasion of privacy:

(a) that the plaintiff had taken reasonable steps, prior to commencing or continuing proceedings, to settle the dispute with the defendant in order to avoid the need for litigation;

(b) that the defendant had not taken reasonable steps to settle the dispute with the plaintiff in order to avoid the need for litigation;

(c) that the defendant's unreasonable conduct at the time of the invasion of privacy or prior to or during the proceedings had subjected the plaintiff to special or additional embarrassment, harm, distress or humiliation;

(d) that the defendant's conduct was malicious or committed with the intention to cause embarrassment, harm, distress or humiliation to the plaintiff; and

(e) that the defendant has disclosed information about the plaintiff which the defendant knew to be false or did not honestly believe to be true.

Proposal 11–4 The new Act should provide that the court may not award a separate sum as aggravated damages.

Proposal 11–5 The new Act should provide that, in an action for serious invasion of privacy, courts may award exemplary damages in exceptional circumstances and where the court considers that other damages awarded would be an insufficient deterrent.

Proposal 11–6 The total of any damages other than damages for economic loss should be capped at the same amount as the cap on damages for non-economic loss in defamation.

Proposal 11–7 The new Act should provide that a court may award the remedy of an account of profits.

Proposal 11–8 The new Act should provide that courts may award damages assessed on the basis of a notional licence fee in respect of the defendant's conduct, in an action for serious invasion of privacy.

Proposal 11–9 The new Act should provide that courts may award an injunction, in an action for serious invasion of privacy.

Proposal 11–10 The new Act should provide that courts may order the delivery up and destruction or removal of material, in an action for serious invasion of privacy.

Proposal 11–11 The new Act should provide that courts may make a correction order, in an action for serious invasion of privacy.

Proposal 11–12 The new Act should provide that courts may make an order requiring the defendant to apologise to the plaintiff, in an action for serious invasion of privacy.

Proposal 11–13 The new Act should provide that courts may make a declaration, in an action for serious invasion of privacy.

Question 11–1 What, if any, provisions should the ALRC propose regarding a court's power to make costs orders?

12. Breach of Confidence Actions for Misuse of Private Information

Proposal 12–1 If a statutory cause of action for serious invasion of privacy is not enacted, appropriate federal, state, and territory legislation should be amended to provide that, in an action for breach of confidence that concerns a serious invasion of privacy by the misuse, publication or disclosure of private information, the court may award compensation for the claimant's emotional distress.

Proposal 12–2 Relevant court acts should be amended to provide that, when considering whether to grant injunctive relief before trial to restrain publication of private (rather than confidential) information, a court must have particular regard to freedom of expression and any other countervailing public interest in the publication of the material.

13. Surveillance Devices

Proposal 13–1 Surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.

Proposal 13–2 Surveillance device laws should include a technology neutral definition of 'surveillance device'.

Proposal 13–3 Offences in surveillance device laws should include an offence proscribing the surveillance or recording of private conversations or activities without the consent of the participants. This offence should apply regardless of whether the person carrying out the surveillance is a participant to the conversation or activity, and regardless of whether the monitoring or recording takes place on private property.

Proposal 13–4 Defences in surveillance device laws should include a defence of responsible journalism, for surveillance in some limited circumstances by journalists investigating matters of public concern and importance, such as corruption.

Question 13–1 Should the states and territories enact uniform surveillance laws or should the Commonwealth legislate to cover the field?

Proposal 13–5 Surveillance device laws should provide that a court may make orders to compensate or otherwise provide remedial relief to a victim of unlawful surveillance.

Question 13–2 Should local councils be empowered to regulate the installation and use of surveillance devices by private individuals?

14. Harassment

Proposal 14–1 A Commonwealth harassment Act should be enacted to consolidate and clarify existing criminal offences for harassment and, if a new tort for serious invasion of privacy is not enacted, provide for a new statutory tort of harassment. Alternatively, the states and territories should adopt uniform harassment legislation

15. New Regulatory Mechanisms

Proposal 15–1 The ACMA should be empowered, where there has been a privacy complaint under a broadcasting code of practice and where the ACMA determines that a broadcaster's act or conduct is a serious invasion of the complainant's privacy, to make a declaration that the complainant is entitled to a specified amount of compensation. The ACMA should, in making such a determination, have regard to freedom of expression and the public interest.

Proposal 15–2 A new Australian Privacy Principle should be inserted into the *Privacy Act 1988* (Cth) that would:

(a) require an APP entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual; and

(b) require an APP entity to take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance.

Question 15–1 Should the new APP proposed in Proposal 15–2 also require an APP entity to take steps with regard to third parties with which it has shared the personal information? If so, what steps should be taken?

Question 15–2 Should a regulator be empowered to order an organisation to remove private information about an individual, whether provided by that individual or a third party, from a website or online service controlled by that organisation where:

(a) an individual makes a request to the regulator to exercise its power;

(b) the individual has made a request to the organisation and the request has been rejected or has not been responded to within a reasonable time; and

(c) the regulator considers that the posting of the information constitutes a serious invasion of privacy, having regard to freedom of expression and other public interests?

Proposal 15–3 The *Privacy Act 1988* (Cth) should be amended to confer the following additional functions on the Australian Information Commissioner in relation to court proceedings relating to interferences with the privacy of an individual:

(a) assisting the court as amicus curiae, where the Commissioner considers it appropriate, and with the leave of the court; and

(b) intervening in court proceedings, where the Commissioner considers it appropriate, and with the leave of the court.

Part 1

1. Introduction

Contents

This Inquiry

1.1 This Inquiry comes at a time of continuing and rapid advances in technology with increasing capacities to affect the privacy of individuals. Many of these technological advances are beneficial to society and are valued by the individuals and organisations that use them or who benefit from their use. However, these technologies also raise concerns about privacy that might once have been the stuff of science fiction but are now based on reality.

1.2 The challenge for lawmakers is how to ensure that the law remains relevant, appropriate and workable in the light of technological advances. By the 1990s technology had already taken a monumental leap with the development and uptake of the internet and the worldwide web and with advances in digital technology.

1.3 Over the last 20 years, governmental, commercial and personal use of digital technology has become universal. Data-mining methods, search engines and data analytics have revolutionised the processing, recognition, communication, acquisition and aggregation of knowledge and information. Mobile technologies and devices have become increasingly affordable to all social and economic strata of society. Social media have transformed interpersonal communications. Media convergence has made today's media a different phenomenon from even its 1990 counterparts.

1.4 The scope of this Inquiry is not confined to invasions of privacy brought about by digital technology. Significant gaps in data protection regulation, deficiencies or inconsistencies in criminal surveillance or harassment laws, and gaps in the existing common law protection against physical invasions of an individual's privacy also underpin the need for a review of the existing law.

1.5 The divergence in the recommendations of previous inquiries into privacy law, significant developments in other jurisdictions, concerns expressed in the community, continuing gaps in Australian common law and statute law protecting privacy, and new

problems raised by the use of rapidly developing technologies[1] all require detailed consideration by the ALRC in this Inquiry.

1.6 This document commences the second stage in the consultation process in this Inquiry into serious invasions of privacy. The first stage included the release of the Issues Paper, *Serious Invasions of Privacy in the Digital Era* (ALRC IP 43, 2013), in response to which the ALRC received many valuable submissions.[2] The Final Report will be provided to the Attorney-General by the end of June 2014.

How to make a submission

1.7 With the release of this Discussion Paper, the ALRC invites individuals and organisations to make a submission, particularly in response to the specific proposals and questions, but also to any of the background material and analysis.

1.8 There is no specified format for submissions, although the questions and proposals may provide useful guidance. Submissions may be made in writing, by email or using the ALRC's online submission form. Submissions made using the online submission form are preferred.

1.9 Generally, submissions will be published on the ALRC website, unless marked confidential. Confidential submissions may still be the subject of a request for access under the *Freedom of Information Act 1982* (Cth). 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.

> Submissions using the ALRC's online submission form can be made at: <www.alrc.gov.au/content/privacy-subs-DP80>.
>
> In order to ensure consideration for use in the Final Report, submissions must reach the ALRC by **Monday 12 May 2014**.

The Terms of Reference

1.10 The Terms of Reference set out and limit the scope of the ALRC's Inquiry. The ALRC is asked to make recommendations on the detailed legal design of a statutory civil cause of action for serious invasions of privacy. The ALRC is also asked to make recommendations about other legal remedies and innovative ways in which the law could prevent or redress serious invasions of privacy. This latter task has required the ALRC to consider how a range of existing common law causes of action and remedies

---

1 M Paterson notes that 'Surveillance in public places has assumed additional importance in the light of technological developments that have taken place since the publication of the VLRC's report in 2010', citing, for example, increased availability of face and number plate recognition and radio frequency identification technologies: M Paterson, *Submission 60*.

2 Both the Issues Paper and this Discussion Paper may be downloaded free of charge from the ALRC website, <www.alrc.gxjov.au>. Hard copies may be obtained on request by contacting the ALRC on (02) 8238 6333. Public submissions are also published on the ALRC website.

and statutory provisions might be strengthened or amended, as well as considering proposals for new ways in which the law could prevent or redress invasions of privacy.

1.11 The Terms of Reference also 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 Discussion Paper addresses this issue at several stages, both in relation to the elements of a statutory cause of action and in relation to existing legal remedies[3] and elsewhere.

Emerging threats to privacy

1.12 Particular attention has been directed recently to the rapidly expanded technological capacity of organisations not only to collect, store and use personal information, but also to track the physical location of individuals, to keep the activities of individuals under surveillance, to collect and use information posted on social media, to intercept and interpret the details of telecommunications and emails, and to aggregate, analyse and sell data from many sources.

1.13 Organisations that may collect and process personal information include:

- national and foreign security organisations;
- government agencies, such as education or health entities or local councils;
- law enforcement agencies;
- media entities;
- financial institutions and credit reporting agencies;
- national and international commercial entities;
- social media platforms;
- retail, marketing and behavioural advertising companies; and
- civilian activist groups.

1.14 Corporate or governmental activities involving the processing of personal information are governed by a range of common law obligations or statutes or regulatory schemes concerned with the collection, storage or dissemination of data or with related matters such as the protection of intellectual, real and personal property, financial interests and reputation.

1.15 Data processing by commercial, government and non-government organisations may often be necessary, appropriate and lawful; carried out with relevant consents or authority or specifically authorised by statute; justified in the public interest; or within the terms and conditions specified by the relevant entity for the provision of a service. Most corporations realise the importance of taking privacy concerns seriously: quite apart from legal reasons, there are important reputational and business consequences of

3 See Ch 12.

data breaches. Many of the organisations described above belong to industry associations which endorse the importance of privacy protection.

1.16 Nonetheless, breaches of privacy do occur as a result of the activities of these organisations for a range of reasons. Some breaches of a person's privacy might be unavoidable; others might come about due to systemic weaknesses in a system of data protection, or through incompetence or lack of care. Some may be caused by deliberate and unpredictable activities of unauthorised third parties, intent on breaking into a data system. Some activities may be outside, or exempt from any existing regulation or law. Some activities may amount to an indefensible, unlawful and deliberate invasion of the privacy of an individual.

1.17 Modern privacy concerns are not however limited to the use of personal information by organisations. Many disputes about invasions of privacy are between individuals. Many of the cases in other jurisdictions involve the conduct of individuals. The ALRC has received submissions from individuals and representative groups concerned about:

- people installing surveillance cameras which can record their neighbour's activities;
- surveillance cameras installed by activists trespassing onto private property and the subsequent posting of the footage on websites; and
- harmful, invasive and distressing disclosure of personal information and images by an individual's former partner.

Previous inquiries and international developments

1.18 This Inquiry builds on four other recent inquiries into privacy law or related issues conducted in Australia, three of which recommended the enactment of a statutory cause of action.[4]

1.19 The ALRC's report, *For Your Information: Privacy Law and Practice* (ALRC Report 108, 2008) focused on data protection: information collection, access and use. The ALRC recommended that Commonwealth legislation should provide for a statutory cause of action for serious invasion of privacy.[5]

1.20 In 2009, the New South Wales Law Reform Commission (NSWLRC) recommended that a general cause of action for invasion of privacy was required to

---

4 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: ALRC, *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 Co-Operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1983: ALRC, *Privacy*, Report No 22 (1983). This resulted in the enactment of the *Privacy Act 1988* (Cth).

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

provide a 'basis for the ongoing development of the law of privacy in a climate of dynamic societal and technological change'.[6]

1.21 In 2010, the Victorian Law Reform Commission (VLRC) issued the report, *Surveillance in Public Places*, which followed a decade-long inquiry into workplace privacy and privacy in public places.[7]

1.22 In September 2011, the Department of the Prime Minister and Cabinet (DPM&C) released an Issues Paper on a statutory cause of action for invasion of privacy,[8] prompted by a number of 'high profile privacy breaches' in Australia and overseas.[9]

1.23 In addition to a continuing debate in Australia on the desirability of a statutory cause of action, there have been important developments in privacy protection in other countries. Privacy torts have been well-established in the United States for many decades, although the protection they provide is limited by the constitutional protection of free speech in the First Amendment of the US Constitution. Some states, such as California, have also introduced a statutory tort of invasion of privacy.[10]

1.24 The United Kingdom has developed extensive legal protection of privacy by extending the equitable action for breach of confidence, under the influence of the *Human Rights Act 1998* (UK).[11] This Act requires the courts to give effect to the protection of rights and freedoms set out in arts 8 and 10 of the *European Covenant on Human Rights.*

1.25 The Canadian provinces of British Columbia,[12] Manitoba,[13] Newfoundland and Labrador,[14] Quebec[15] and Saskatchewan[16] have enacted statutory torts for invasion of privacy, and the Ontario Court of Appeal has also recognised common law protection.[17] New Zealand courts have recently recognised common law torts of misuse of private information[18] and of intrusion.[19]

1.26 The state of development of a country's common law protection of privacy has a significant impact on the question of whether there is a need to legislate for a cause of action. Committees in both the United Kingdom and New Zealand have recommended

---

6 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) [4.14].
7 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010).
8 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, 2011).
9 This presumably referred 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).
10 *California Civil Code* § 1708.8.
11 *Campbell v MGN Ltd* [2004] 2 AC 457. See Ch 12.
12 *Privacy Act*, RSBC 1996, c 373.
13 *Privacy Act*, RSM 1987, c P125.
14 *Privacy Act*, RSNL 1990, c P-22.
15 *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35–37.
16 *Privacy Act*, RSS 1978, c P-24.
17 *Jones v Tsige* (2012) 108 OR (3rd) 241.
18 *Hosking v Runting* (2005) 1 NZLR 1.
19 *C v Holland* [2012] 3 NZLR 672 (24 August 2012).

against the introduction of a statutory cause of action, in view of the common law developments in those two countries.[20]

1.27 In contrast, a common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility of such a development, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*.[21] While a tort of invasion of privacy has been recognised by two lower court decisions,[22] no appellate court has confirmed the existence of this tort. The general consensus is that the likely direction of the future development of the common law is uncertain.[23]

Should a new cause of action be enacted?

1.28 The ALRC considers that the question of whether a statutory cause of action for serious invasion of privacy would be beneficial to the Australian community is best answered after considering:

- the existing legal protections for privacy;
- the gaps in that legal protection identified;
- the precise elements of the proposed cause of action; and
- any alternative ways in which the unacceptable gaps in the law might be filled.

1.29 Only a very few stakeholders who made submissions to the Inquiry told the ALRC that the law did not need to be changed at all, and that there were no gaps in the legal protection of privacy in Australia.[24] Those who opposed the introduction of a new cause of action recognised the gaps in the law, but submitted that it would be preferable to fill those gaps in other ways.[25] Many other stakeholders expressed their support for a statutory cause of action. Both stakeholders who supported and those who opposed the introduction of a new cause of action made submissions as to the desirable elements of any such action.

1.30 The cause of action proposed in this Discussion Paper is more precise than similar privacy actions recommended in other law reform reports, and in some respects more narrow. The ALRC believes that precision is important so that stakeholder groups, individuals and lawmakers can reach a more informed view on the potential interpretation and application of the proposed action, on the extent of protection it may provide to potential claimants, and on the impact it may have on those who would face potential liability. Only when these assessments are made can there be an informed

---

20 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); New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3*, Report No 113 (2010).

21 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

22 *Grosse v Purvis* [2003] QDC 151 (16 June 2003); *Doe v Australian Broadcasting Corporation* [2007] VCC 281. Both cases were settled before appeals by the respective defendants were heard.

23 The case law on the issue since *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* is discussed in Ch 3.

24 Free TV, *Submission 55*; The Newspaper Works, *Submission 50*.

25 SBS, *Submission 59*; AIMIA Digital Policy Group, *Submission 56*; News Corp Australia, *Submission 34*.

debate on the relative desirability of the proposed statutory cause of action or other alternatives.

1.31 Privacy law must recognise other values and interests, such as freedom of expression. This is reflected in the design of the tort proposed in this Discussion Paper. While this may mean that one interest is not as protected or as unconstrained to the extent some advocates would prefer, the ALRC considers that the law may be able to find a middle ground where a balance can be reached and a degree of useful protection can be enacted.

1.32 The statutory cause of action is thus directed at serious invasions of privacy committed intentionally or recklessly with no countervailing justification or defence. If the statute provides remedies for such invasive conduct, Australia will have made an important and clear step in providing greater protection for privacy than is currently available. It will give Australians the privacy protections enjoyed by those in other countries, including the UK, New Zealand and Canada.

1.33 The statutory cause of action is not, however, the only way that greater protection could be achieved by statutory reform. This Discussion Paper, in Part 3, suggests other measures that should be considered to improve the protection in Australia of people's privacy in the digital age, some in addition to and some as an alternative to a new statutory cause of action.

2. Guiding Principles

Contents

Summary

2.1 The Issues Paper identified several principles for guiding the recommendations for reform in this Inquiry into serious invasions of privacy.

2.2 There was wide support by stakeholders for these principles. Some stakeholders suggested additional matters that should be incorporated into the principles; some argued that certain principles should be given greater emphasis or priority; others stressed that there should be no hierarchy or preference for certain interests.

2.3 The principle which elicited the strongest support was that the protection of privacy must be balanced with other fundamental freedoms and matters of public interest.

2.4 The Guiding Principles are not the only considerations that will underpin any legislative reforms, but they generally accord with established values and concepts that have been set out in discussions about the legal protection of privacy. The discussion of the value, importance and role of privacy in various contexts and from various perspectives—legal, philosophical, social, political, technical—is extensive. This Discussion Paper does not attempt to survey these discussions or the enormous body of literature on the topic. Rather, this chapter identifies some key considerations that will underpin the recommendations to be made in the Final Report.

2.5 The Guiding Principles draw on leading cases in Australia and other jurisdictions, international conventions, academic commentary on privacy and related fields, the Terms of Reference, and similar principles identified in earlier ALRC reports and submissions to this Inquiry.

Principle 1: Privacy is a fundamental value worthy of legal protection

2.6 Privacy is important to enable individuals to live a dignified, fulfilling, safe and autonomous life. It is an important element of the fundamental freedom of individuals that underpins their:

- ability to form and maintain meaningful and satisfying relationships with others, including intimate and family relationships;
- freedom of speech, thought and self-expression;
- freedom of movement and association;
- ability to engage in the democratic process;
- freedom to engage in secure financial transactions;
- freedom to develop and advance their own intellectual, cultural, artistic, property and physical interests; and
- freedom from undue interference or harm by others.

2.7 The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* (ICCPR) and other international instruments and treaties.[1] Article 17 of the ICCPR, to which Australia is a signatory, provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[2]

2.8 Many stakeholders stressed the importance of privacy to a person's autonomy and rights of self-determination.[3] The Law Institute of Victoria, for example, noted that 'the protection of an individual's privacy is fundamental to their human dignity and is central to many other human rights such as the right of freedom of association, movement and expression'.[4]

2.9 Privacy also gives individuals greater freedom to pursue their cultural interests free from undue interference from others. This freedom may be particularly important for some ethnic, religious and cultural groups, such as Aboriginal and Torres Strait

---

1 *Convention on the Rights of the Child*, opened for signature 20 December 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16; *Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*, opened for signature 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003) art 14.

2 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

3 See, eg, Electronic Frontiers Australia, *Submission 44*; A Johnston, *Submission 9*; I Pieper, *Submission 6*.

4 Law Institute of Victoria, *Submission 22*.

Islander people, who have particular cultural identity, knowledge and customs that bear on the privacy interests of individuals within the group.[5]

2.10 Some representative groups also stressed the importance of a right to privacy for protecting vulnerable individuals in the community from undue interference or harassment, or the fear of violence and harassment by others.[6] Privacy plays an important role in ensuring personal safety and freedom from harassment.

2.11 As privacy is about individual freedoms, corporate entities, government organisations or agencies, and elected groups would not have a right of action to sue for invasion of privacy under the ALRC's proposals.[7] This is consistent with the common law, which recognises that privacy is a matter of human dignity and sensitivity.[8] This does not deny the possibility of invasions of the privacy of persons within a corporate entity or other organisation, nor the right of corporate entities to sue at common law for interference with their property rights.

Principle 2: There is a public interest in protecting privacy

2.12 This principle reflects the long-held acceptance by the law that the notion of public interest does not simply comprise matters in which the public as a whole has a communal interest, such as the proper administration of government or the proper administration of justice. Rather, there is also a public interest in the protection and enforcement of private freedoms and rights of individuals. This is embodied in the law's protection of information imparted under a contractual or equitable obligation of confidence.[9] A similar concept underpins the protection of many property and possessory rights.[10]

2.13 It follows that in many cases involving the protection of privacy, the court will not only be concerned to provide a remedy that will protect the individual litigant. Courts will also be concerned to provide a remedy that will have a normative effect on the behaviour of others in the community, either by way of deterrent or example, so providing a measure of protection to a broader class of people. Legal rights can help set standards of behaviour, and may be valuable even if those rights are not often enforced.

2.14 Privacy, like confidentiality, underpins other important individual freedoms. Privacy and the ability to speak freely without fear of disclosure is important for social order and public health, private wellbeing, and the achievement of many social ideals and objectives. Without privacy and confidentiality, a person may feel unsafe or unable

---

5 Arts Law Centre of Australia, *Submission 43*.

6 Women's Legal Services NSW, *Submission 57*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*.

7 NSW Young Lawyers, *Submission 58*; Blueprint for Free Speech, *Submission 26*.

8 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [43] (Gleeson CJ).

9 On the public interest in upholding confidences, see *Prince of Wales v Associated Newspapers Ltd* [2007] 3 WLR 222, [67]. See further Ch 12.

10 'If the courts of common law do not uphold the rights of individuals by granting effective remedies, they invite anarchy, for nothing breeds social disorder as quickly as the sense of injustice which is apt to be generated by the unlawful invasion of a person's rights': *Plenty v Dillon* (1991) 171 CLR 635, 655 (Gaudron and McHugh JJ).

to speak freely and honestly about an important matter, such as a suspicion about criminal activity, a problem about one's own or another person's activities, or a health concern about a condition, disease or substance addiction. There is also a public interest in the security of confidential information about an individual's financial and commercial interests.

2.15 The public interest in confidentiality and privacy is reflected in many legal principles, such as the defence of qualified privilege in defamation law, or in the approach of the courts in granting injunctions to constrain the breach of a contractual or equitable obligation of confidence.[11] It is also reflected in legislative provisions dealing with the confidentiality of medical records and medical information about a person.[12]

Principle 3: Privacy should be balanced with other important interests

2.16 The privacy of an individual is not an absolute value or right which necessarily takes precedence over other values of public interest. As stakeholders noted, it must be balanced with a range of other important values, freedoms and matters of public interest, including, in no particular order or hierarchy:

- freedom of speech,[13] including the freedom of the media and the implied constitutional freedom of political communication;[14]
- freedom of artistic and creative expression and innovation in the digital era;[15]
- 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 and the apprehension of criminals;[16]

---

11 This point is discussed further in Ch 12.

12 See, eg, *Public Health Act 2010* (NSW) s 130.

13 In *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3 (27 February 2013) French CJ sets out a useful summary of the ways in which freedom of speech as a value underpins much of Australian common law and statute law.

14 RSPCA, *Submission 49*. The RSPCA submission referred to *ABC v Lenah Game Meats*, where Kirby J suggests that courts should give a wider interpretation than they have done to date on the matters falling within the implied freedom: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 286–287.

15 Facebook, *Submission 65*.

16 For example, in 2012–2013, information obtained under communications interception or stored communications warrants was used in 3,083 arrests, 6,898 prosecutions and 2,765 convictions: Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979: Annual Report 2012–2013* (2013) 4. Other submissions referring to the importance of detecting criminal or fraudulent activity included Australian Federal Police, *Submission 67*; Google, *Submission 54*; CV Check, *Submission 23*; Insurance Council of Australia, *Submission 15*.

- the effective delivery of essential and emergency services in the community;[17]
- the protection of vulnerable persons in the community;
- national economic development and participation in the global digital economy;[18] and
- the value of individuals being enabled to engage in digital communications and electronic financial and commercial transactions.[19]

2.17 This list is not an exhaustive list of public interest matters. Some stakeholders emphasised the need for a holistic approach to the balancing of interests in particular circumstances,[20] while others stressed the need for the balancing process to consider the degree to which any interference with one interest was necessary and proportionate to the protection of the other. This latter concept is stressed in privacy litigation in the United Kingdom since the introduction of the *Human Rights Act 1998* (UK), and is also relied upon in European case law dealing with the *European Convention on Human Rights*.[21]

2.18 There was widespread support among stakeholders for the articulation of this principle, and no stakeholders submitted that privacy should be regarded as an absolute right. Stakeholders suggested the following additions to the above list:

- the public's right to be informed on matters of public importance, in real time rather than after delay,[22] and to have access to publicly available information and accurate historical records;[23]
- the need for transparency in government, corporate and organisational dealings or operations that affect individuals;[24] and
- the desirability of Australian businesses being able to compete in the global economy and to encourage innovation and business in Australia.[25]

---

17 Australian Communications and Media Authority, *Submission 52*.
18 Australian Bankers' Association, *Submission 27*.
19 CV Check, *Submission 23*.
20 Electronic Frontiers Australia, *Submission 714*; B Arnold, *Submission 28*.
21 *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).
22 Australian Subscription Television and Radio Association, *Submission 47*.
23 Arts Law Centre of Australia, *Submission 43*; Australian Institute of Professional Photography, *Submission 31*; Public Interest Advocacy Centre, *Submission 30*. It should be noted that some limitations on public access to historical records already exist. For example, under s 33(1)(g) of the *Archives Act 1983* (Cth) the National Archives of Australia is authorised to withhold information from public access if the release of that information would unreasonably disclose information relating to the personal affairs of an individual.
24 Pirate Party of Australia, *Submission 18*.
25 Google, *Submission 54*; Telstra, *Submission 45*; Optus, *Submission 41*.

Principle 4: Australian privacy laws should meet international standards

2.19 The protection of privacy in Australia should be consistent with Australia's international obligations, for example, under the ICCPR[26] and policies of the Organisation for Economic Co-operation and Development.[27] It should also take into account, as far as appropriate, international standards and legal developments in the protection of privacy.[28]

2.20 Throughout this Discussion Paper, reference is made to developments in the legal protection of privacy in other jurisdictions, particularly but not limited to those jurisdictions with which Australia shares a common legal heritage. However, the Discussion Paper recognises that every jurisdiction's development of the law on privacy will depend on its constitutional framework, particularly its guarantees or protections of relevant interests or rights.[29] The need for statutory reform in a particular jurisdiction also depends on its common law at the time.

Principle 5: Privacy laws should be adaptable to technological change

2.21 The design of legislative protections of privacy should be sufficiently flexible to adapt to rapidly changing technologies and capabilities without the need for constant amendments. At the same time, they should be drafted with sufficient precision and definition to promote certainty as to their application and interpretation.

2.22 Several stakeholders stressed the need for law reform to be technologically neutral to avoid the risk of becoming outdated by rapid developments in technology.[30] For example, Google submitted that there is a need for flexible, forward-looking and adaptive data policies to ensure that society may benefit from the many beneficial uses of data analytics.[31]

Principle 6: Privacy laws should be clear and certain

2.23 A key concern in relation to the introduction of a statutory cause of action for serious invasion of privacy is uncertainty as to how the various provisions of a statute

---

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

27 Organisation for Economic Co-Operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013.

28 Australian Bureau of Statistics, *Submission 32*.

29 SBS, *Submission 59*.

30 Google, *Submission 54*; Australian Communications and Media Authority, *Submission 52*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Optus, *Submission 41*; Australian Privacy Foundation, *Submission 39*; Australian Bureau of Statistics, *Submission 32*; C Jansz-Richardson, *Submission 24*; CV Check, *Submission 23*; Law Institute of Victoria, *Submission 22*.

31 Google, *Submission 54*.

would be interpreted and applied by courts in the future. Some stakeholders stressed the benefits of precision, clarity and certainty.[32]

2.24 The ALRC agrees that, where possible, the law should be precise and certain, but also flexible and able to adapt to changes in social and technological conditions. The ALRC is also mindful, however, that Parliament cannot legislate precisely for all the different situations that may arise in the future and that certain issues must be left to the courts to determine in the light of all the circumstances of a particular case. Stakeholders pointed out that judges are used to deciding the types of issues that will arise in privacy cases, such as the existence and weight of public interest.[33] Where appropriate, the ALRC suggests some guidance on the relevant factors the court might or should consider.[34]

2.25 The ALRC has specifically addressed the desirability of precision and certainty in its detailed legal design of the proposed statutory cause of action, but the principle underpins all of the ALRC's recommendations.

Principle 7: Privacy laws should be coherent and consistent

2.26 Any recommendation for a statutory cause of action for serious invasion of privacy (or other remedy) should promote coherence in the law and be consistent with other Australian laws or regulatory regimes. Recommendations should also promote uniformity or consistency in the law throughout Australian jurisdictions.

2.27 In its consultations and other occasions,[35] the ALRC has heard of widespread concern, uncertainty and confusion caused by notable differences in the law between the various states and territories. Two obvious examples relating to privacy are the inconsistency of legislation dealing with the use of surveillance devices and with harassment and cyber-bullying.

2.28 Inconsistent laws not only provide poor protection for privacy, but also inadequately protect countervailing interests—such as freedom of the media. Victims of unauthorised surveillance are poorly protected if they are unable to determine if a breach of a statute has occurred. The important activities of others, such as media entities, which operate nationally, may be overly restricted if it is unclear when and where they might be breaching a law.[36] The ALRC's recommendations are directed at achieving legal uniformity across Australia in relation to many different types of invasions of privacy.

---

32 Telstra, *Submission 45*; C Jansz-Richardson, *Submission 24*.

33 For example, B Arnold submitted that 'Australian jurisprudence regarding confidentiality, defamation and national security has demonstrated that courts are fully capable of identifying public interest and of dealing with tensions in claims regarding public good': B Arnold, *Submission 28*.

34 See, for example, Ch 8.

35 Standing Committee on Social Policy and Legal Affairs, *Roundtable on Drones and Privacy*, 28 February 2014, Parliament House, Canberra.

36 Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*.

2.29 The need for coherence and consistency also underlies the desirability of avoiding unnecessary overlap between legal regimes. Many stakeholders[37] expressed the view that any proposed remedial regime should not overlap or be inconsistent with the various regulatory schemes[38] and statutory prohibitions that already constrain the activities of certain organisations and render them subject to substantial compliance requirements, enforceable obligations, civil penalties, and private law remedies. This was a particular concern in view of the new compliance requirements imposed on entities as a result of amendments to the *Privacy Act 1988* (Cth) (*Privacy Act*) that came into force in March 2014.

2.30 However, regulation, the criminal law and the civil law can serve different purposes, even if they overlap in some ways. As discussed in Chapter 3, there are many different regulatory regimes, criminal laws and civil obligations and remedies protecting people from breaches or invasions of privacy either directly or indirectly. Any proposal for law reform should be considered in the context of the whole range of existing laws.

2.31 The consequence of a breach of a regulatory scheme or of the criminal law may not result in any personal remedy to a person affected by the breach. In some cases, this may be appropriate, as the person affected may be one of thousands of people affected and the individual may have not have suffered any material or serious harm. In this case, a more appropriate response may be a regulatory scheme that ensures that such a breach does not happen again. The breach may also lead to a criminal prosecution that may punish the perpetrator, and deter such conduct in the future.

2.32 Finally, legal reforms affecting civil liability for invasions of privacy should be consistent with legislative policy as it affects civil liability for wrongs to others generally,[39] and with other common law principles, unless there is an express and clear intent to override or distinguish them.

Principle 8: Justice to protect privacy should be accessible

2.33 The law should provide a range of means to prevent, reduce or redress serious invasions of privacy and it should facilitate appropriate access to justice for those affected.

---

37 Australian Federal Police, *Submission 67*; Google, *Submission 54*; ABC, *Submission 46*; Telstra, *Submission 45*; Optus, *Submission 41*.

38 The key existing regulatory schemes include those under the *Privacy Act 1988* (Cth), legislation dealing with health information, and state and territory legislation on data protection, outlined in Ch 3. In addition, commercial activities are regulated by the *Australian Competition and Consumer Act 2010* (Cth) and similar state legislation, and banks by various statutes and regimes that govern financial institutions. Further, such organisations are often subject to a range of civil obligations to their customers in contract, tort law or equitable principles, while tort and equitable obligations also arise where there is no contract between the parties.

39 For example, the policy implicit in the civil liability legislation in most states, and in the common law, limiting liability for negligently inflicted mental harm to plaintiffs suffering a recognised psychiatric illness.

2.34 Many stakeholders submitted that any statutory cause of action or other remedy for serious invasions of privacy should be accessible to people with limited means as well as to those who can more easily afford the high costs of litigation.[40] The law should also make appropriate provision for people with disability or others who require assistance in obtaining access to justice.[41]

2.35 There is also widespread support for an approach that will encourage or make available a range of flexible and accessible alternative dispute resolution mechanisms.[42]

Principle 9: Privacy protection is an issue of shared responsibility

2.36 The notion of shared responsibility is an important consideration informing legislative frameworks for the protection of privacy. Provided they have the power and means to do so, individuals bear a measure of responsibility for the protection of their own privacy and the privacy of others. Organisations that collect, store, process, or disclose information have a responsibility to empower individuals to control their own personal information as much as practicable and appropriate, but also to take steps to protect the privacy of individuals. Legislative and non-legislative mechanisms are needed to ensure that individuals can and that organisations do adequately exercise their respective responsibilities to protect privacy.

2.37 The ALRC considers that capable adults should be encouraged to take reasonable steps to utilise the privacy tools and frameworks offered by service providers. Several stakeholders stressed the importance of personal responsibility. The Australian Federal Police, for example, argued that 'individuals should take ownership of their own privacy'.[43] The National E-Health Transition Authority (NEHTA) advanced the concept of personal control, arguing that individuals can and should exercise control over their electronic health records. NEHTA explained that this control may be exercised through individuals setting controls over access to their health records; authorising others to access their records; and the capacity to make enquiries and complaints about the treatment of their online records.[44]

---

40 Office of the Australian Information Commissioner, *Submission 66*; Australian Communications and Media Authority, *Submission 52*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Optus, *Submission 41*; Australian Bureau of Statistics, *Submission 32*; Public Interest Advocacy Centre, *Submission 30*; CV Check, *Submission 23*; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*.

41 Office of the Public Advocate (Queensland), *Submission 12*. Representative actions are discussed in Ch 9.

42 Office of the Australian Information Commissioner, *Submission 66*; Women's Legal Services NSW, *Submission 57*; ABC, *Submission 46*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Interactive Games and Entertainment Association, *Submission 40*; Australian Privacy Foundation, *Submission 39*; C Jansz-Richardson, *Submission 24*; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*; Pirate Party of Australia, *Submission 18*; I Pieper, *Submission 6*. Alternative dispute resolution is discussed in Ch 9.

43 Australian Federal Police, *Submission 67*.

44 National E-Health Transition Authority, *Submission 8*.

2.38 However, personal responsibility can only be fully exercised when individuals are provided with the tools necessary to protect their privacy, and when the choices expressed by individuals are respected. Personal responsibility of individuals must therefore be balanced with the responsibility of organisations and service providers. Service providers should provide transparent and accessible methods to protect the privacy of their customers. This includes providing clear privacy policies, information about how to protect privacy, and privacy warnings, where relevant. Individuals need to be kept properly informed if privacy policies are not followed or are to be unilaterally changed.

2.39 Several stakeholders made submissions stressing the role of education as an essential and powerful tool to prevent invasions or breaches of privacy that might arise from the use of the internet or digital and mobile technologies.[45] Many people of all ages are unaware of the means available to protect their privacy, of the risks to privacy that arise in the digital era, and of the legal ramifications of some conduct.

2.40 The ALRC considers that education has an important role to play in reducing and preventing serious invasions of privacy, particularly in assisting individuals to interact safely and effectively in online and electronic relationships—whether they are personal or commercial in nature—and to respect the privacy of others. The ALRC considers that governments and industry have a responsibility to provide adequate education and assistance, particularly for vulnerable members of the Australian community, such as people with disability, children and some young people who may lack the capacity or knowledge to effectively protect their privacy in the digital era.

2.41 To that end, the ALRC highlights the responsibility of governments, relevant industries and industry groups representing entities that benefit from the advances of the digital era, to fund and support education programs which provide assistance and advocacy for individuals to manage their privacy. The ALRC has not made any proposals regarding education, as the ALRC's Terms of Reference for this Inquiry are limited to consideration of the ways in which the law may redress and reduce serious invasions of privacy.

---

45 Australian Federal Police, *Submission 67*; Facebook, *Submission 65*; Google, *Submission 54*. Google submitted that: 'The ALRC's Issues Paper is focused for the most part on what *legal* reforms are appropriate to protect privacy in the digital era. Google believes, however, it would be a missed opportunity for the ALRC not to consider the important role of non-legislative measures such as education in empowering individuals to protect their own privacy online'.

3. Overview of Current Law

Contents

Summary

3.1 As background to the proposals in this Discussion Paper, this chapter sets out a brief survey of the existing legal regulation and remedies that protect people's privacy in Australia. The existing legal protection of privacy in Australia takes many forms. Protection of privacy interests of individuals can be found in regulatory schemes, criminal laws and civil or private law.

3.2 This is followed by a brief summary of the main gaps or deficiencies in the way that Australian law prevents or redresses serious invasions of privacy. In the ALRC's view, the existing law is a patchwork, with some important pieces missing and inconsistencies between others.

Information privacy

3.3 The *Privacy Act* is Australia's key information privacy law.[1] It is concerned with the security of personal information held by certain entities, rather than with privacy more generally.[2]

3.4 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.[3] The APPs bind only 'APP entities'—primarily Australian Government agencies and large private sector organisations with a turnover of more than $3 million. Certain small businesses are also bound, such as those that provide health services and those that disclose personal information to anyone else for a benefit, service or advantage.[4] Generally, individuals are not bound by the *Privacy Act*.[5]

3.5 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.

3.6 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.[6]

3.7 The *Privacy Act* provides several complaints paths for individuals where there has been (or is suspected to have been) a breach of an APP. The primary complaints process is through a complaint to the Australian Information Commissioner, initiating an investigation by the Commissioner.[7] This process typically requires that the individual has first complained to the relevant APP entity.[8] An investigation may result in a determination by the Commissioner, containing a declaration that:

- the respondent's conduct constituted an interference with the privacy of an individual and must not be repeated or continued;

---

1 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 by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), key provisions of which came into effect on 14 March 2014.

2 Confusion about the role and scope of the *Privacy Act* might be avoided if it were renamed to, for example, the *Information Privacy Act* or the *Data Protection Act*. These titles are used for similar Acts in the UK and Canada, and would more accurately reflect the remit of the Australian *Privacy Act*. The ALRC previously made such a recommendation in ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 5–3.

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

4 'APP entity' is defined in Ibid s 6(1). Small businesses are not, in general, APP entities, with some exceptions as set out in s 6D.

5 There are some exceptions. For example, an individual who is a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), will be treated as an APP entity under the *Privacy Act 1988* (Cth).

6 *Privacy Act 1988* (Cth) s 13G.

7 Ibid ss 36, 40.

8 Ibid s 40(1A).

- the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;
- the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
- the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- that no further action is needed.[9]

3.8 A complainant may apply to the Federal Court of Australia or the Federal Circuit Court of Australia to enforce a determination of the Commissioner.[10]

3.9 An individual may also apply to the Federal Court or Federal Circuit Court for an injunction where a person has, is, or is proposing to engage in conduct that was or would be a breach of the *Privacy Act*.[11] This path appears to have been used relatively infrequently.[12]

3.10 The *Privacy Act* also grants a range of powers to the Australian Information Commissioner, including the power to:

- investigate complaints made by individuals or on the Commissioner's own motion about APP entities;[13]
- direct agencies to conduct privacy impact assessments;[14] and
- apply for Federal Court and Federal Circuit Court orders for civil penalties for serious or repeated breaches of the APPs.[15]

3.11 State and territory legislation creates information privacy 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.[16]

3.12 The existing Commonwealth, state and territory legislation applies to major organisations that collect and store personal information, such as banks, large retailers, government departments and utilities providers. There are a large number of

---

9 Ibid s 52(1).
10 Ibid s 55A.
11 Ibid s 98.
12 The ALRC is aware of only two successful applications: *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* [2004] FCA 637 (21 May 2004); *Smallbone v New South Wales Bar Association* [2011] FCA 1145 (6 October 2011).
13 *Privacy Act 1988* (Cth) pt V.
14 Ibid s 33D.
15 Ibid s 80W.
16 *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). The *Privacy Act 1988* (Cth) has application to agencies in the Australian Capital Territory.

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.[17]

3.13 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 to two years.

Health information privacy

3.14 Health and genetic information is recognised as 'sensitive information' under the *Privacy Act*. Sensitive information is given greater protection under the APPs than other information.[18] Separate Commonwealth Acts protect healthcare identifiers[19] and electronic health records.[20]

3.15 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.[21]

Communications privacy

3.16 The *Telecommunications Act 1997* (Cth) (*Telecommunications Act*) prohibits the disclosure of certain information by telecommunications providers.[22] Contravention of these prohibitions is an offence punishable by up to two years imprisonment.[23]

3.17 There are a number of exceptions, for example, for disclosures to ASIO or the Australian Federal Police, under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). Exceptions also exist for disclosure under the authority of an 'authorised officer' of an enforcement agency,[24] but this does not permit the disclosure of the contents or substance of a communication.[25] An authorised officer must consider the privacy of any person before making an authorisation.[26]

---

17 *Privacy Act 1988* (Cth) s 6C.

18 'Sensitive information' is defined in Ibid s 6(1). A number of the APPs make special provisions for sensitive information: see, eg, APP 3.

19 *Healthcare Identifiers Act 2010* (Cth).

20 *Personally Controlled Electronic Health Records Act 2012* (Cth).

21 *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).

22 *Telecommunications Act 1997* (Cth) pt 13.

23 Ibid s 276(3).

24 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 171–182.

25 Ibid s 172. A disclosure under these provisions is therefore limited to telecommunications data ('metadata').

26 Ibid s 180F.

3.18 The TIA Act prohibits the unauthorised access of communications, subject to various exceptions,[27] unless a warrant is obtained.[28] Those who issue warrants must consider, among other things, the privacy of persons affected by the access.[29]

3.19 The TIA Act also prohibits the unauthorised interception of communications over a telecommunications system, again, subject to various exceptions,[30] unless a warrant is obtained.[31] Those who issue an interception warrant must consider, among other things, the privacy of persons affected by the interception.[32]

Surveillance laws and laws affecting photography

3.20 Legislation exists in each of the states and territories that variously restricts the use of listening, optical, data and tracking surveillance devices. These surveillance device laws provide criminal offences for using a surveillance device to record or monitor private conversations or activities, for tracking a person or for monitoring information on a computer system.[33] The surveillance device laws also place restrictions on communicating information obtained through the use of a surveillance device.

3.21 The surveillance device laws of each state and territory differ greatly, both in terms of the types of surveillance devices they regulate, and the circumstances in which those surveillance devices may or may not be used. For example, the laws of Victoria, Queensland and the Northern Territory permit a participant to record a private activity in the absence of the consent of other parties, while the remaining surveillance device laws do not.[34]

3.22 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.[35] Once again there are inconsistencies between these laws, and such laws only exist in three jurisdictions (the ACT, NSW and Victoria).

3.23 Criminal laws in some—but not all—jurisdictions provide for offences relating to photography being used for indecent purposes[36] or indecent filming without

---

27 Ibid s 108.
28 Ibid ss 110–132.
29 Ibid s 116(2).
30 Ibid s 7.
31 Ibid ss 9–18, 34–61A.
32 Ibid ss 46(2), 46A(2).
33 *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *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).
34 See Ch 13.
35 *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).
36 *Summary Offences Act 1988* (NSW) s 4; *Criminal Code Act 1899* (Qld) s 227(1); *Police Offences Act 1935* (Tas) s 13.

consent.[37] Criminal laws also provide protection against indecent photography of children in private and public places.[38] In each case, the laws are restricted to specific subject matter, for example, matter of a sexual nature; filming for specific purposes, for example, for sexual gratification; or filming of a particular type of person, for example, a child. These laws therefore provide limited general privacy protection.

3.24 The operation of the *Privacy Act 1988* (Cth) is restricted to the actions of government agencies and big business, not the activities of individuals acting in a personal capacity such as freelance or amateur photographers. However the Act does regulate the activities of individuals, agencies and companies which 'disclose personal information about another individual to anyone else for a benefit, service or advantage'.[39] This may provide scope to regulate the actions of photographers who take unauthorised photographs of individuals.[40]

Harassment and stalking offences

3.25 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'[41] or by 'otherwise contacting the victim'.[42]

3.26 The Commonwealth *Criminal Code Act 1995* provides offences for conduct amounting to harassment that occurs via a communications service (which includes the internet). Relevant offences include 'using a carriage service to menace, harass or cause offence'[43] and 'using a carriage service to make a threat'.[44]

3.27 There is a strong framework in family law to protect individuals from harassment, including harassment that occurs via electronic communications. However, this is limited to the victims of family violence.[45]

Industry codes and guidelines

3.28 Various statutory and self-regulatory bodies oversee and enforce industry codes and guidelines which protect against invasions of privacy.

3.29 Commercial television and radio broadcasters are subject to a self-regulatory scheme under the *Broadcasting Services Act 1992* (Cth). Commercial broadcasting

---

37 *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.

38 See, for example, *Criminal Law Consolidation Act 1935* (SA) s 63B.

39 *Privacy Act 1988* (Cth) s 6D(4)(c),(d).

40 Ibid s 6: The definition of 'record' includes 'a photograph or other pictorial representation of a person'.

41 *Crimes Act 1958* (Vic) s 21A(2)(b).

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

43 *Criminal Code Act 1995* (Cth) s 474.17.

44 Ibid s 474.15.

45 For example, stalking is included in the definition of 'family violence' in the *Family Law Act 1975* (Cth) s 4AB(2)(c).

industry codes of practice include provisions relating to the protection of privacy.[46] The ABC and SBS are each subject to a separate code of practice; each of these codes also contains provisions relating to the protection of privacy.[47] The Australian Communications and Media Authority (the ACMA) has oversight of each of these codes of practice, however the ACMA has limited enforcement powers where a code is breached.

3.30 The Australian Press Council oversees its members' compliance with its *Charter of Press Freedom* (2003) and *Statement of Privacy Principles* (2011).

3.31 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.

Existing common law causes of action

3.32 There are a number of existing causes of action at common law which can, in some cases, be used to protect privacy or have the effect of protecting personal privacy.[48] These causes of action protect against physical intrusions upon, and surveillance of, a person and against unauthorised disclosure of private information.

Physical intrusions

3.33 Trespass to the person and trespass to land provide some protection against unauthorised interference with a person's body or intrusions into property.[49] Both forms of the ancient tort of trespass are actionable per se, meaning that the tort is actionable when the interference occurs, without the need for the claimant to establish any recognised form of damage such as personal injury, psychiatric illness, property damage or economic loss.

3.34 'General' damages, sometimes substantial, are awarded to compensate the claimant for the wrong that has occurred, and for any actual damage sustained, or by way of solace or vindication of his or her rights.[50] Aggravated damages may be awarded where there is a special humiliation of the claimant by the defendant. Exemplary or punitive damages may be awarded where the defendant has acted intentionally or maliciously and in arrogant or contumelious disregard of the claimant's

46 Commercial Television Industry Code of Practice 2010 cl 4.3.5; Commercial Radio Codes of Practice and Guidelines 2011 cl 2.1(d).
47 ABC Code of Practice 2011 cl 6.1; SBS Codes of Practice 2014 cl 1.9.
48 C Sappideen and P Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) ch 26.
49 Living in modern society automatically exposes a person to the risk of everyday forms of contact, and consent to this contact can be inferred: *Collins v Wilcock* (1984) 1 WLR 1172.
50 *Plenty v Dillon* (1991) 171 CLR 635, [654]–p655] (Gaudron and McHugh JJ).

rights.[51] Claimants may seek injunctions to restrain the broadcast of video material recorded without authorisation while a defendant was trespassing on land,[52] although damages have been deemed an adequate remedy in cases involving commercial enterprises.[53]

3.35 However, both forms of trespass require a physical interference (or a threat of physical interference in the case of trespass to the person) and will therefore not apply to a person who merely follows or watches or keeps a person under surveillance without any threat, or who remains outside the land to carry out surveillance.

3.36 Trespass to land also has strict requirements as to the title over the land that the claimant must have in order to sue in trespass. Thus, someone who is on the land under a mere contractual or other licence, for example, the hire of premises for a wedding[54] or the occupation of a hospital bed or room,[55] will not have a sufficient right to exclusive occupation of the land or premises to sue in trespass for an invasion of privacy into that space. Finally, trespass to land has no operation where the claimant is in a public space and complains that there has been intrusion into his or her private activities, affairs or seclusion.

Surveillance from outside a property

3.37 A person may be liable in the tort of nuisance for an unreasonable interference with an occupier's use and enjoyment of his or her land,[56] for example by keeping the occupier under surveillance or by positioning cameras or lights in situations where they interfere with, record or 'snoop' on the occupier's activities.[57] Again, only the occupier with a right to exclusive possession may sue in nuisance and the cause of action has been denied to other lawful occupants of the land who may be there under licence from the occupier. This characterisation of other occupants as mere licensees has even been applied to family members of the lawful occupier.[58]

Intrusions into airspace

3.38 Intrusions into airspace may amount to trespass to land if the intrusion is at a height potentially necessary for the ordinary use and enjoyment of the occupier[59] and, in the case of aircraft, if the intrusion does not come within the protection provided by legislation dealing with the mere flight of aircraft through airspace. For example, s 72(1) of the *Civil Liability Act 2002* (NSW) provides that 'no action lies in respect of trespass or nuisance by reason only of the flight (or the ordinary incidents of the flight)

---

51 *XI Petroleum (NSW) Pty Ltd v Caltex Oil (Australia) Pty Ltd* (1985) 155 CLR 448.

52 *Emcorp Pty Ltd v Australian Broadcasting Corporation* [1988] 2 Qd R 169.

53 *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457; *Brigthen Pty Ltd v Nine Network Australia Pty Ltd* [2009] NSWSC 319 (2009).

54 *Douglas v Hello! Ltd* [2005] EWCA Civ 595 (18 May 2005).

55 *Kaye v Robertson* [1991] FSR 62.

56 RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) ch 14.

57 *Raciti v Hughes* (1995) 7 BPR 14837. The plaintiffs successfully obtained an injunction to prevent the use of motion-triggered lights and surveillance cameras aimed at their backyard.

58 *Hunter and Others v Canary Wharf Ltd; Hunter and Others v London Docklands Corporation* [1997] AC 655; *Oldham v Lawson (No 1)* [1976] VR 654.

59 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 495.

of an aircraft over any property at a height above the ground that is reasonable (having regard to wind, weather and all the circumstances of the case) so long as the Air Navigation Regulations are complied with'.[60] These provisions were originally enacted in most jurisdictions in the 1950s to protect the then young commercial airline industry. Arguably, they were not directed at the sort of technological intrusions possible today, such as by the use of unmanned aerial devices or drones.

3.39 It is a question of fact in the circumstances as to whether or not a trespass has occurred on common law principles. This would depend on whether the potential use and enjoyment of the land and the airspace by the occupier has been interfered with from within the relevant height limit of the occupier's interests.[61] If the interference was from outside the occupier's airspace, the circumstances could amount to a nuisance at common law.

3.40 In the case of aircraft, it would additionally depend on whether or not the height of the intrusion is reasonable in all of the circumstances.[62] Mere compliance with Air Navigations Regulations, which are aimed at safety issues,[63] would not necessarily excuse the use of an aircraft to interfere with the occupier's use or enjoyment of the land or the occupier's privacy or that of the occupier's guests.[64] Aerial photography, recording and surveillance carried out from a plane or helicopter or drone may therefore amount to a trespass to land or a nuisance, but there is a dearth of case authority dealing with these types of intrusion.

3.41 In *Bernstein v Skyviews*, the defendant photographed the plaintiff's property from a flight many hundreds of feet above the property for the purpose of offering to sell the photographs to the plaintiff. The plaintiff was unsuccessful in this case. However, Griffiths J said:

> I [would not] wish this judgment to be understood as deciding that in no circumstances could a successful action be brought against an aerial photographer to restrain his activities. The present action is not founded in nuisance for no court would regard the taking of a single photograph as an actionable nuisance. But if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief.[65]

Defamatory publications

3.42 The tort of defamation provides redress for a person whose reputation is damaged by a publication to a third party. Until the enactment of uniform *Defamation*

---

60 *Civil Liability Act 2002* (NSW) s 72(1).

61 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 495; *Lord Bernstein v Skyviews and General Ltd* [1978] 1 QB 479, 489. See also *Bocardo SA v Star Energy UK Onshore Ltd* [2010] 3 ER 975, [984]–[993].

62 See, eg, *Civil Liability Act 2002* (NSW) s 72(1). A similar provision applies in the United Kingdom: *Lord Bernstein v Skyviews and General Ltd* [1978] 1 QB 479.

63 Civil Aviation Safety Authority, *Submission 2*.

64 *New South Wales v Ibbett* (2006) 229 CLR 638; *Halliday v Neville* (1984) 155 CLR 1, 8.

65 *Lord Bernstein v Skyviews and General Ltd* [1978] 1 QB 479, 489.

Acts in 2005 in Australian states and territories,[66] defamation law provided considerable indirect[67] protection of private information because in some states defendants could only justify a defamatory publication by showing not only its truth but also that it was published in the public interest or for the public benefit.[68] However, the truth of the defamatory statement is now a complete defence, so that the action provides much more limited protection of privacy.[69]

Disclosures of confidential information

3.43 The equitable action for breach of confidence has long been a key source of protection against the misuse or disclosure of confidential information. Confidential information is information which is not generally or publicly known but is only known to a deliberately restricted number of individuals.

3.44 The action was originally confined to information that had been imparted in circumstances expressly or impliedly imposing an obligation of confidence. Sometimes this obligation arises under contract, with normal contractual remedies flowing from the breach, including, in limited cases, damages for mental distress. But the courts of equity also recognised the obligation outside contract—for example, as to personal details imparted in a close personal relationship,[70] although they might refuse relief where the parties had already been very public about their relationship.

3.45 It is now well accepted in the United Kingdom[71] and Australia[72] that an obligation of confidence may arise where a party comes into possession of information which he or she knows, or ought to know, is confidential. This extension of the law makes the equitable action for breach of confidence a powerful legal weapon to protect individuals from the unauthorised disclosure of confidential information.

3.46 However, as discussed in Chapter 12, there is still some uncertainty in Australia as to what compensation is available in an equitable action for breach of confidence.

Unauthorised photography

3.47 Generally speaking, there is no common law right not to be photographed that can be exercised to prevent photography or filming of someone in a public place without his or her consent.[73] There is also no prohibition on taking photographs of private property from public land, unless the conduct amounts to stalking or the intent

---

66 *Civil Law (Wrongs) Act 2002* (ACT) ch 9; *Defamation Act 2005* (NSW); *Defamation Act 2006* (NT) 2006; *Defamation Act 2005* (SA); *Defamation Act 2005* (Qld) 2005; *Defamation Act 2005* (Tas); *Defamation Act 2005* (Vic); *Defamation Act 2005* (WA).

67 *Australian Consolidated Press Ltd v Ettingshausen* [1993] NSWCA (13 October, 1993).

68 *John Fairfax Publications Pty Ltd v Hitchcock* [2007] NSWCA 364 (14 December 2007) [124].

69 Sappideen and Vines, above n 48, ch 25.

70 *Argyll v Argyll* (1965) 1 ER 611.

71 *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109.

72 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 224, Gleeson CJ.

73 '[A] person, in our society, does not have a right not to be photographed': *R v Sotheren* [2001] NSWSC 204 (16 March 2001) [25] (Dowd J).

is to 'peep or pry' on an individual.[74] Private property owners or public entities such as local councils, educational institutions or museums may regulate photography on private property or places they control, by the express terms on which entry is authorised. In other cases, a lack of authority to enter for the purpose of taking photographs or recordings may be inferred.[75]

Gaps in existing law

3.48 Although the existing law provides protection against some invasions of privacy, there are significant gaps or uncertainties. These include the following:

- The tort actions of trespass to the person, trespass to land and nuisance do not provide protection from unauthorised and serious intrusions into a person's private activities in many situations.[76] The statutory cause of action for serious, unjustified invasions of privacy committed intentionally or recklessly, detailed in Chapters 4–11, or the proposals in Chapter 14 relating to harassment, would supplement the common law.
- Outside actions of trespass, malicious prosecution or defamation, tort law does not provide a remedy for intentional infliction of emotional distress which does not amount to psychiatric illness.[77] The proposed statutory cause of action would allow recovery of damages for emotional distress caused by a serious invasion of privacy. In Chapter 12, the ALRC has proposed that, if a statutory cause of action for serious invasion of privacy is not enacted, legislation should be enacted that would provide for the recovery of damages for emotional distress in breach of confidence cases.
- While the equitable action for breach of confidence can provide effective legal protection to prevent the disclosure of private information (and especially if the Australian common law develops as it has in the UK), it is currently less effective after a wrongful disclosure, because it is unclear or uncertain whether a plaintiff may recover compensation for emotional distress. Proposal 12–1 in Chapter 12 aims to remove this uncertainty.
- There is further uncertainty, or at least some debate, as to the relevant principles to be applied when a court is considering whether to grant an interlocutory injunction to restrain the publication of true, private information.[78] Chapter 12 includes Proposal 12–2 that would require courts to give consideration to freedom of expression and matters of public interest when considering such an injunction.

---

74 See, for example, *Crimes Act 1900* (NSW) s 547C.

75 *Halliday v Neville* (1984) 155 CLR 1, 8; *TCN Channel Nine Pty Ltd v Anning* (2002) 54 NSWLR 333.

76 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.

77 *Wainwright v Home Office* [2004] 2 AC 406; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.

78 The guidance provided by defamation cases such as *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57 and by cases on protection of confidential information is of uncertain application in view of the potentially different interests in privacy actions.

- Legislation dealing with surveillance and with workplace surveillance is not uniform throughout Australia, and is outdated in some states. The ALRC has proposed in Chapter 13 that these surveillance device laws should be made uniform.
- There is no tort or civil action for harassment, nor is there sufficient deterrence against 'cyber-harassment' in Australian law, compared with overseas jurisdictions.[79] The ALRC has made proposals in Chapter 14 for civil remedies and criminal penalties for harassment if a statutory cause of action for serious invasion of privacy is not enacted.[80]
- Legislation and common law protection against aerial and other surveillance may not provide sufficient protection against advances in technology that facilitate new types of invasion into personal privacy.[81] This limitation would be addressed by the statutory cause of action for serious invasions of privacy. In addition, the proposals in Chapter 13 for the reform of state and territory surveillance devices Acts would regulate new means of surveillance.
- The *Privacy Act* and state and territory equivalents deal only with information privacy. Further, the *Privacy Act* provides for only limited civil redress, that is, only by way of a complaints procedure to the Office of the Australian Information Commissioner (OAIC). While important, this legislation by no means covers the field of invasions of privacy. For example, it does not deal with intrusions into personal privacy or with the behaviour of most individuals or with most activities of media entities.
- The ACMA cannot provide any monetary redress to those who complain about invasions of privacy by media or communications entities. There is a proposal in Chapter 15 for the ACMA to be given limited powers to redress complaints of serious unjustified invasions of privacy, similar to those of the OAIC.
- Many small businesses, those with an annual turnover of less than $3 million, are exempt from the regulatory regime of existing privacy legislation. The small business exemption is discussed in Chapter 15.

3.49 The ALRC is not able, in the time allocated to this Inquiry, to consider and make recommendations about all of the concerns that have been raised by the community in relation to privacy in the digital era. This Discussion Paper sets out the key proposals to which, in the light of its Terms of Reference, the ALRC has given priority for consideration.

---

79 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 2013* (SNS), c2 criminalises cyber-bullying.

80 See Ch 14 and in particular Proposal 14–1.

81 An example is the increasing use of unmanned aerial vehicle (drones) to carry out unauthorised aerial surveillance.

3.50 Some of the concerns that are raised in the community are more properly dealt with by existing regulatory bodies. Some of the concerns have been the subject of recent, carefully considered enactment by Parliament, for example, the recent amendments to the *Privacy Act* by the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), many of which came into effect only in March 2014.

3.51 Further, there have been a number of targeted reviews for existing legislation which is the subject of community debate. The privacy protections of *Telecommunications Act* and the TIA Act were the subject of a 2013 Parliamentary Inquiry.[82] At the time of writing, a further Parliamentary Inquiry is underway.[83] The ALRC does not consider these provisions in this Inquiry.

A common law action for breach of privacy in Australia?

3.52 A common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility of such a development in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* in 2001.[84] A tort of invasion of privacy has been recognised by two lower court decisions: *Grosse v Purvis* in the District Court of Queensland[85] and *Doe v Australian Broadcasting Corporation*[86] in the Country Court of Victoria. Both cases were settled before appeals by the respective defendants were heard. No appellate court has confirmed the existence of this tort.

3.53 Commenting on *Grosse v Purvis*, Heerey J in *Kalaba v Commonwealth of Australia* held that the weight of authority was against the proposition that the tort is recognised at common law.[87] In *Chan v Sellwood; Chan v Calvert,* Davies J described the position on the existence of the tort at common law as 'a little unclear'.[88] In *Gee v Burger*, McLaughlin AsJ considered the matter 'arguable'.[89]

3.54 In *Giller v Procopets*,[90] the Supreme Court of Victoria Court of Appeal found it unnecessary to consider whether the tort of invasion of privacy exists at common law, having upheld the plaintiff's claim on the basis of the equitable action for breach of confidence.

---

82 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* 2013.

83 Legal and Constitutional Affairs References Committee, *Comprehensive Revision of Telecommunications (Interception and Access) Act 1979* (referred by Senate on 12 December 2012; Reporting Date 10 June 2014).

84 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

85 *Grosse v Purvis* [2003] QDC 151 (16 June 2003). See also, Des A Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 352.

86 *Doe v Australian Broadcasting Corporation* [2007] VCC 281 (2007).

87 *Kalaba v Commonwealth of Australia* [2004] FCA 763 (8 June 2004) 6.

88 *Chan v Sellwood; Chan v Calvert* [2009] NSWSC 1335 (9 December 2009) [34].

89 *Gee v Burger* [2009] NSWSC 149 (13 March 2009) [53].

90 *Giller v Procopets* (2008) 24 VR 1.

3.55 In *Dye v Commonwealth Securities Ltd,* Katzmann J noted 'that it would be inappropriate to deny someone the opportunity to sue for breach of privacy on the basis of the current state of the common law'.[91]

3.56 In *Maynes v Casey*, Basten J, with whom Allsop P agreed, referring to *Australian Broadcasting Corporation v Lenah Game Meats* and *Giller v Procopets*, said that 'These cases may well lay the basis for development of liability for unjustified intrusion on personal privacy, whether or not involving breach of confidence', but held that the facts as found were against the plaintiff.[92] The trial judge had concluded that he did not consider the defendant's conduct 'to be an undue or serious invasion of any right to privacy possessed by the plaintiffs or to be highly offensive to a reasonable person of ordinary sensibility'.[93]

3.57 In *Saad v Chubb Security Australia Pty Ltd*, Hall J in the NSW Supreme Court considered a claim brought by the plaintiff against her employer and the security firm engaged to monitor the workplace, after CCTV images of the plaintiff at work were posted on a Facebook site, probably by an employee or former employee of the security firm. Ball J refused to strike out a claim for breach of confidence, holding 'I do not consider that, at this stage of the proceedings, it is open to conclude that the cause of action for breach of confidence based on invasion of the plaintiff's privacy would be futile or bad law'.[94]

3.58 In *Sands v State of South Australia*, 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'.[95]

3.59 Recently in *Doe v Yahoo!7 Pty Ltd,* Smith DCJ said, 'it seems to me there is an arguable case of invasion of privacy. … I would be very hesitant to strike out a cause of action where the law is developing and is unclear'.[96]

3.60 The general consensus then is that the likely direction of the future development of the common law is uncertain.

---

91 *Dye v Commonwealth* [2010] FCA 720 [290]. However, Katzmann J refused leave to the plaintiff to amend her pleadings to include such a claim, on various grounds.
92 *Maynes v Casey* [2011] NSWCA 156 (14 June 2011) [35].
93 *Maynes v Casey* [2010] NSWDC 285 (23 December 2010) [195].
94 *Saad v Chubb Security Australia Pty Ltd* [2012] NSWSC 1183 [183].
95 *Sands v State of South Australia* [2013] SASC 44 (5 April 2013) [614].
96 *Doe v Yahoo!7 Pty Ltd* [2013] QDC 181 (9 August 2013) [310]–[311].

Part 2

4. A New Tort in a New Commonwealth Act

Contents

Summary

4.1 This chapter sets out the ALRC's proposals for how a statutory cause of action for serious invasion of privacy should be set in the context of existing laws.

4.2 The ALRC proposes that the statutory cause of action be contained in a new, stand-alone Commonwealth Act. Including the new action in a Commonwealth Act would ensure consistency in the operation of the cause of action throughout Australia.

4.3 The new cause of action should be set out in a new Act, rather than the *Privacy Act 1988* (Cth). The *Privacy Act* largely concerns information privacy, while the new cause of action is designed to remedy a number of different types of invasions of privacy, including physical invasions of privacy.

4.4 The ALRC proposes that a statutory cause of action for serious invasion of privacy should be a tort. If the statutory cause of action were a tort, there would be increased certainty around various ancillary matters, such as vicarious liability. There would also be the benefit of more consistency, since the statutory cause of action would operate in concert with existing tort law.

4.5 Finally, this chapter provides an overview of the elements of the statutory cause of action that are set out in Chapters 5–8. In discussing the elements of the statutory cause of action, it is important to consider these elements together. There are significant interactions between the elements, and the ALRC's reasons for proposing the content of one proposal will therefore often depend on the ALRC's proposals for the other elements.

A new stand-alone Commonwealth Act

Proposal 4–1 A statutory cause of action for serious invasion of privacy should be contained in a new Commonwealth Act (the new Act).

4.6 The ALRC considers that if a statutory cause of action were to be introduced, it should be in Commonwealth legislation, as this is the best way to ensure the action is available and consistent throughout Australia. It is often difficult to achieve consistency across state and territory legislation. Inconsistent statutory provisions in state and territory legislation would be highly confusing and create unnecessary complexity in the law. This would also provide poor protection of privacy generally and have a damaging effect on many other activities that are of significant public interest. Inconsistency and complexity of legislation would increase costs for businesses, particularly those operating across state and international boundaries. Difficult questions of jurisdiction and applicable law would arise. There would also be a risk of 'forum shopping' if the details of the cause of action differed between Australian jurisdictions.

4.7 The ALRC considers that the cause of action should be in a stand-alone Act to avoid confusion and to enhance clarity.[1] The remedial response to invasions of privacy under the statutory cause of action would be distinct from the regulatory regime which is the essence of the *Privacy Act.*

4.8 The essential purposes and scope of the two regimes are different. The *Privacy Act* sets up a regime for the security and privacy of personal information which is collected, stored or used by certain entities (often known as 'data protection' regulation). The cause of action relates not only to the privacy of information but also to other types of privacy, such as physical privacy.

4.9 The *Privacy Act* sets up a regime to ensure compliance with a number of Australian Privacy Principles (APPs). There is a complaints mechanism which may lead to compensation being paid for an interference with privacy by an act or practice relating to personal information in a manner set out in the Act.[2] However, breaches of the requirements of the *Privacy Act* generally lead to regulatory responses by the Office of the Australian Information Commissioner (OAIC), including the possible imposition of civil penalties on the relevant entity.[3] An invasion of privacy that is actionable under the new Act would lead only to a range of civil remedies sought by and for the benefit of the plaintiff.

---

1 This was also the view in ALRC Report 108, which stated that 'there may be significant confusion arising from the placement of the cause of action in that Act [the *Privacy Act*]. For example, whether the exemptions under the Privacy Act applied to the cause of action, and the interaction between the cause of action and other complaint mechanisms, may be unclear if the *Privacy Act* were amended to include the cause of action': ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [74.195].

2 The complaints mechanism is discussed in Ch 15.

3 These responses are outlined in Ch 3.

4.10 Lastly, the *Privacy Act* is limited in its application to certain entities across Australia. It does not apply to most individuals,[4] or to state agencies. It also includes a number of exemptions, such as for small businesses and media organisations, which would have no application to the new statutory cause of action. The new statutory cause of action would apply, subject to jurisdictional limitations and any defences, to any person or entity that seriously invades the privacy of a person in the circumstances set out in the Act.

4.11 Therefore, the ALRC considers that the new tort should be located in a new stand-alone Commonwealth Act. This new Act might be called the *Serious Invasions of Privacy Act*.

4.12 The location of a statutory cause of action in a separate Commonwealth Act would not prevent power being given to the OAIC to determine complaints concerning conduct that fell within the cause of action by relevant entities. The current complaints regime under the *Privacy Act 1988* could be broadened to encompass such conduct by relevant entities, to provide complainants with an alternative to court proceedings in respect of the conduct.

Constitutional issues

Head of power

4.13 This section examines the scope of the Commonwealth's power to legislate with respect to privacy under the *Constitution*. This issue was previously discussed in the ALRC's report, *For Your Information: Privacy Law and Practice* (ALRC Report 108, 2008).[5]

4.14 The Commonwealth has the power to make laws with respect to 'external affairs'.[6] This power enables the Commonwealth to implement obligations under a bona fide treaty.[7] It is open to the legislature to decide the means by which it gives effect to those obligations, but those means must be 'reasonably capable of being considered appropriate and adapted to that end'.[8]

4.15 Australia is a State Party to the *International Covenant on Civil and Political Rights* (ICCPR). Australia ratified the ICCPR on 13 November 1980. Article 17 of the *ICCPR* provides:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.

---

4 As noted in Ch 3, the *Privacy Act* does apply to some individuals, such as individuals who operate certain types of businesses, such as businesses that trade in personal information: see ss 6C–6EA of the *Privacy Act*. Section 16 of the *Privacy Act* provides that the APPs do not apply to personal information that is collected, used, held or disclosed by an individual in connection with the individual's family or household affairs.

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [3.17]–[3.28].

6 *Constitution* s 51(xxix).

7 *Commonwealth v Tasmania* (1983) 158 CLR 1.

8 *Victoria v Commonwealth ('The Industrial Relations Act case')* (1996) 187 CLR 416, 487 (Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ).

> (2) Everyone has the right to the protection of the law against such interference or attacks.

4.16 In light of the Commonwealth's power to implement treaty obligations under s 51(xxix), it is likely that a law which created a statutory cause of action for serious invasion of privacy would be valid as a means of giving effect to Australia's obligation under art 17 of the *ICCPR*.

4.17 The ALRC considers that the enactment of a statutory cause of action for serious invasion of privacy satisfies the requirement of proportionality. It is 'reasonably capable of being considered appropriate and adapted' to implementing art 17 of the ICCPR. The courts grant latitude to Parliament in selecting the means by which to give effect to a treaty obligation.[9] Moreover, art 17(2) of the *ICCPR* explicitly provides that the protection of law should be afforded to those subject to interference with or attacks on their privacy. Therefore, the law conforms to the treaty and carries its provisions into effect.[10]

4.18 The ALRC noted in 2008 that the current *Privacy Act 1988* (Cth) is purportedly enacted on the basis of the external affairs power.[11] In addition, the ALRC canvassed other heads of power, which may also support aspects of the statutory cause of action.[12] One of these was the Commonwealth's power to legislate with respect to 'postal, telegraphic, telephonic and other like services'.[13] This head of power has been interpreted broadly.[14] The technology-neutral phrase 'other like services' demonstrates that the possibility of developments in technology was contemplated by drafters when framing section 51(v).[15] Radio and television broadcasting have been held to be within the Commonwealth's power under s 51(v).[16] Although the Commonwealth's power to regulate the internet under this head of power is yet to be considered by the High Court, it is likely that it would be a 'like service'.[17]

4.19 If the Commonwealth does enact a statutory cause of action, it may expressly or impliedly 'cover the field' on the subject matter. Any State Act which was inconsistent with the Commonwealth Act would be inoperative.[18]

Constitutional limits

4.20 The Commonwealth's power to legislate is subject to both express and implied constitutional limitations.

---

9 Leslie Zines, *The High Court and the Constitution* (Butterworths, 4th ed, 1997) 288.
10 *Richardson v Forestry Commission* (1988) 164 CLR 261, 345 (Gaudron J).
11 *Privacy Act 1988* (Cth) Preamble.
12 *Constitution* s 51(i), (v), (xiii), (xiv), (xx).
13 *Constitution* s 51(v).
14 *Jones v Commonwealth (No 2)* [1965] HCA 6 (3 February 1965).
15 *Grain Pool of Western Australia v Commonwealth* (2000) 202 CLR 479, 493.
16 *R v Brislan; Ex parte Williams* (1935) 54 CLR 262; *Jones v Commonwealth (No 2)* (1965) 112 CLR 206.
17 Helen Roberts, 'Can the Internet be Regulated?' (Research Paper No 35, Parliamentary Library, Parliament of Australia, 1996) 25.
18 *Constitution* s 109.

Implied freedom of political communication

4.21 The legislative power of the Commonwealth is subject to the implied freedom of political communication. In assessing whether a law infringes the freedom, there are two questions:

> 1. Does the law effectively burden freedom of communication about government or political matters in its terms, operation or effect?
>
> 2. If the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end in a manner which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government and the procedure prescribed by s 128 of the Constitution for submitting a proposed amendment to the Constitution to the informed decision of the people?[19]

A law will only infringe the implied freedom if the answer to the first question is 'yes' and the answer to the second question is 'no'.

4.22 The ALRC considers that the proposed statutory cause of action would not infringe the implied freedom of political communication. The proposed cause of action requires that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest. The freedom of expression includes the freedom to discuss governmental matters. It is likely that the cause of action is 'reasonably appropriate and adapted' to serve a legitimate end, that is, the protection of privacy, in a manner compatible with the maintenance of representative and responsible government.

Impact on States

4.23 The ALRC's 2008 report discussed the *Melbourne Corporation* principle, as an implied limitation on the Commonwealth's power to legislate. Most recently, the High Court expressed the *Melbourne Corporation* principle as concerned with

> whether impugned legislation is directed at States, imposing some special disability or burden on the exercise of powers and fulfilment of functions of the States which curtails their capacity to function as governments.[20]

4.24 The ALRC considers that a statutory cause of action, while imposing a burden on State agencies, would not curtail the States' capacity to function as governments.

An action in tort

Proposal 4–2 The cause of action should be described in the new Act as an action in tort.

---

19 *Monis v The Queen* (2013) 87 ALJR 340; [2013] HCA 4, [61] (French CJ).

20 *Fortescue Metals Group Ltd v Commonwealth* (2012) 247 CLR 486, [130] (Hayne, Bell and Keane JJ). French CJ, Crennan and Kiefel JJ agreed with the joint reasons on this issue in separate judgments: [6], [145], [229]. See also *Austin v Commonwealth* (2003) 215 CLR 185.

4.25 There are a number of reasons for the proposal that the new cause of action should be an action in tort.

4.26 First, and most importantly, describing the statutory cause of action as a tort action will provide certainty, and prevent disputes arising, about a number of ancillary issues that will inevitably arise. Courts frequently have to decide whether a particular statute gives rise to an action in tort for the purposes of determining whether other consequences follow at common law or under other statutes.[21] This will also be the case if a new statutory cause of action is enacted. For example:

- At common law, an employer is vicariously liable where an employee has injured a third party by a tort committed in the course of employment.[22] It may be relevant to decide whether an employer is vicariously liable to the claimant, in addition to an employee, where the employee is liable under the statutory cause of action.
- At common law, the applicable law for intra-Australian and international torts depends on the place where the tort was committed.[23]
- Many legislative provisions refer to liability in tort. For example, some Australian jurisdictions impose an obligation on an employer to indemnify an employee in respect of 'liability incurred by the employee for the tort' to a third party where the tort occurred in the course of employment.[24] Statutory contribution rights may apply only to 'tortfeasors'.[25]

4.27 Describing the action as a tort action will thus avoid many consequential questions arising once primary liability is established. The cause of action will be more fully integrated into existing laws than if it were simply described as a cause of action. This will also avoid the need for numerous specific provisions dealing with these ancillary issues, adding undesirable length to the legislation.[26]

4.28 Secondly, classifying a civil action for redress which leads to monetary compensation as a tort, is consistent with accepted legal classifications. Defining what is a tort precisely, exhaustively and exclusively is a surprisingly difficult task. Leading

---

21 *Commissioner of Police v Estate of John Edward Russell* (2002) 55 NSWLR 232, [62]–[78] (Spigelman CJ); *Hampic Pty Ltd v Adams* [1999] NSWCA 455 [61]. See also *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB) (16 January 2014); cf *Douglas v Hello! Ltd (No 3)* [2006] QB 125 [96].

22 Lewis Klar, 'Vicarious Liability' in Caroline Sappideen and Prue Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) ch 19.

23 *John Pfeiffer Pty Ltd v Rogerson* (2000) 203 CLR 503; *Regie Nationale des Usines Renault SA v Zhang* (2002) 210 CLR 491. It is not always an easy task to determine the place of the tort: M Davies, AS Bell and PLG Brereton, *Nygh's Conflict of Laws in Australia* (LexisNexis Butterworths, 2010) 425.

24 *Employees Liability Act 1991* (NSW) s 3; *Law Reform (Contributory Negligence and Apportionment of Liability) Act 2001* (SA) s 6(9)(c); *Law Reform (Miscellaneous Provisions) Act 1956* (NT) s 22A.

25 See, for example, *Law Reform (Miscellaneous Provisions) Act 1946* (NSW) s 5.

26 However, as seen below, special provision is made with respect to the limitation period and defences. It may also be preferable to make specific provision for vicarious liability to avoid the kind of dispute that arose in *New South Wales v Bryant* [2005] NSWCA 393 and *Canterbury Bankstown Rugby League Football Club Ltd v Rogers* (1993) Aust Torts Reps 81-246, deriving in part from the conflicting views of Kitto J and Fullagar J in *Darling Island Stevedoring and Lighterage Co Ltd v Long* (1957) 97 CLR 36 as to whether the employer is vicariously liable for the acts or the torts of an employee.

texts tend to answer the question in relatively general terms. *Fleming's The Law of Torts*, for example, defines a tort as 'an injury other than a breach of contract, which the law will redress with damages', but then goes on that 'this definition is far from informative'.[27] Torts may be created by common law or statute.[28]

4.29 Definitions of 'tort' often contain two key features. First, a tort is a civil (as opposed to a criminal) wrong, which the law redresses by an award of damages. Secondly, the wrong consists of a breach of an obligation, often in negative terms such as not to harm or interfere with the claimant, imposed by law (rather than by agreement). But neither of those factors is exclusive to tort law and neither is always borne out, as most texts go on to discuss.

4.30 Nevertheless, liability for conduct invading the privacy of another is analogous to, and will often co-exist with, other torts protecting people from interferences with fundamental rights. Situating the cause of action within tort law will allow the application of common law principles settled in analogous tort claims, particularly in relation to fault, defences and the award of damages and assessment of remedies, where these matters are not set out in the new Act. This will enhance the coherence and consistency of the law.

4.31 Thirdly, the nomenclature of tort is consistent with developments in comparable jurisdictions and would allow Australian courts to draw on analogous case law from other jurisdictions, thus reducing uncertainty and complexity. The four Canadian provinces which have enacted legislation for invasions of privacy describe the relevant conduct as 'a tort'.[29] The New Zealand courts have recognised new causes of action in tort to protect privacy.[30] Developments in the United Kingdom derive from the extension of the equitable action for breach of confidence under the influence of the *Human Rights Act 1998* (UK). However, the misuse of private information giving rise to the extended or new cause of action in the United Kingdom is increasingly referred to as a 'tort'.[31] While Australian courts may not be prepared to take the same leap in classification as may have occurred there, the legislature is not so constrained.

---

27 Prue Vines, 'Introduction' in Caroline Sappideen and Prue Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) 3.

28 KM Stanton et al, *Statutory Torts* (Sweet & Maxwell, 2003) 6: 'Indeed, the only answer [to the question "What is a Tort?"] may be to say that a compensation right is of a tortious character if it is generally regarded as tortious … the phrasing of the statute is likely to play a large part in the classification of rights'.

29 *Privacy Act*, RSBC 1996, c 373 (British Columbia); *Privacy Act*, CCSM 1996, c P125 (Manitoba); *Privacy Act*, RSS 1978, c P-24 (Saskatchewan); *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador).

30 *Hosking v Runting* (2005) 1 NZLR 1; *C v Holland* [2012] 3 NZLR 672 (24 August 2012).

31 *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB) (16 January 2014) [50]–[75]. Many commentators now use this nomenclature: eg, Richard Clayton and Hugh Tomlinson, 'The Human Rights Act and Its Impact on the Law of Tort' in TT Arvind and Jenny Steele (eds), *Tort Law and the Legislature: Common Law, Statute, and the Dynamics of Change* (Hart Publishing, 2012) 466–467. However, precisely when and how this change from an extended equitable action for breach of confidence to a tort of misuse of private information happened has not been pinpointed. Some judicial statements simply ignore the difference: eg, Lord Neuberger, MR, in *Tchenguiz v Imerman (Rev 4)* [2010] EWCA Civ 908 [65]: 'following … *Campbell*, there is now a tort of misuse of private information: as Lord Phillips of Worth Matravers MR put it in *Douglas v Hello! Ltd (No 3)* [2006] QB 125. Cf *Coogan v News Group Newspapers Ltd* [2012]

4.32 Fourthly, describing the action as a tort action will clarify and highlight the distinctions between the statutory cause of action for serious invasion of privacy and existing regulatory regimes, such as those under the *Privacy Act 1988* (Cth) and the *Broadcasting Services Act 1992* (Cth).

4.33 Fifthly, describing the statutory cause of action as a tort action will clearly differentiate it from the equitable and contractual actions for breach of confidence. These will continue to exist and develop to protect confidential information, against the contracting party or confidant and against a third party who has the requisite knowledge that the material is confidential.[32] Lastly, there is no reason why the tort nomenclature should constrain the legislature from making specific provision for remedies not generally available in tort at common law, for example, ordering an apology or an account of profits; limiting remedies usually available in tort; or capping the amounts of certain types of damages.

4.34 In 2009, the New South Wales Law Reform Commission (NSWLRC) recommended against identifying the statutory cause of action as an action in tort, or leaving the courts to construe the action as one in tort. It gave two reasons. First, tort actions do not generally require courts to engage in the sort of overt balancing of interests involved in the statutory cause of action.[33] However, in the ALRC's view this point seems to overlook or downplay the balancing that is required in some existing tort actions. Tort actions in private nuisance frequently require the courts to balance the interests of the plaintiff with those of the defendant in their respective use of their land.[34] Nuisance law famously rests on 'a rule of give and take, live and let live', according to the well-known aphorism of Baron Bramwell in *Bamford v Turner* in 1860.[35] In *Sedleigh Denfield v O'Callaghan*, Lord Wright made a point that would be apt in many cases involving alleged invasions of privacy and the balancing of individuals' rights:

> A balance has to be maintained between the right of the occupier to do what he likes with his own, and the right of his neighbour not to be interfered with. It is impossible to give any precise or universal formula, but it may broadly be said that a useful test is

EWCA Civ 48; [2012] 2 WLR 848 [48] where he said: 'it is probably fair to say that the extent to which privacy is to be accommodated within the law of confidence as opposed to the law of tort is still in the process of being worked out.' Possibly, such detail is of less concern to English courts than it would be to Australian courts, where a stricter approach to the classification of legal wrongs is evident: *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* (2007) 230 CLR 89; *Bofinger v Kingsway Group Ltd* (2009) 239 CLR 269.

32 *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 224–225; *Vestergaard Frandsen A/S and Ors v Bestnet Europe Ltd and Ors* [2013] 1 WLR 1556; *AMI Australia Holdings Pty Ltd v John Fairfax Publications Pty Ltd* [2010] NSWSC 1395.

33 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [5.55].

34 Compare 'Equitable principles are best developed by reference to what conscionable behaviour demands of the defendant not by "balancing" and then overriding those demands by reference to matters of social or political opinion': *Smith Kline and French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* [1990] FCA 151 [130] (Gummow J).

35 *Bamford v Turner* (1860) 3 B & S 62; 122 ER 25 [83]–[84].

> perhaps what is reasonable according to the ordinary usages of mankind living in society.[36]

4.35 Secondly, the NSWLRC said that describing the cause of action as a tort would require the legislation to specify whether the cause of action requires fault on the defendant's part. Further, if it did require fault, what kind of fault, and whether it requires proof of harm or is actionable per se. The NSWLRC considered that the issue of fault was 'appropriately left to development in case law' and that it was unnecessary to specify whether the action is maintainable only on proof of damage.[37] The VLRC agreed with this approach, adding that 'there is little to be gained—and many complex rules of law to be navigated—if any new cause of action is characterised as a tort'.[38] Examples given were rules as to fault, damage, remedies and vicarious liability.

4.36 The ALRC considers that it is highly desirable, if not essential, that the legislator should determine whether or not the cause of action requires proof of a certain type of fault and harm. To leave such key elements of a statutory cause of action to be decided by the courts would be highly problematic. An absence of specificity would increase uncertainty as to the statute's application. This has been a key concern of stakeholders in relation to previous proposals for a statutory cause of action.[39] People need to have some guidance in advance as to when their activities might be judged to be an actionable invasion of privacy leading to civil liability. Similarly, potential claimants need guidance as to whether they could prove an actionable invasion of their privacy. The comments by the European Court of Human Rights in 1966 on the law of the United Kingdom in a different context are apposite:

> The relevant national law must be formulated with sufficient precision to enable the persons concerned—if need be with appropriate legal advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[40]

4.37 If no element of fault is included, it would be open for a court to determine that strict liability was intended or imposed, as for example under ss 18 and 237 of the Australian Consumer Law.[41] The ALRC considers that strict liability, or negligence based liability, would be oppressive or undesirable. Certainty is also desirable in relation to the issue of damage or actionability per se. Questions will undoubtedly arise as to other ancillary issues on liability. The ALRC proposes the integration of the statutory action into the existing legislative and common law framework of tort law.

---

36 *Sedleigh Denfield v O'Callaghan* [1940] AC 880, 903. See also, RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [14.19].

37 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [5.56]–[5.57].

38 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) 7.134.

39 Free TV, *Submission 55*; The Newspaper Works, *Submission 50*; Australian Subscription Television and Radio Association, *Submission 47*; Telstra, *Submission 45*; Australian Bankers' Association, *Submission 27*.

40 *Goodwin v United Kingdom* (1996) 22 EHRR 123, 140. See David Eady, 'Injunctions and the Protection of Privacy' (2010) 29 *Civil Justice Quarterly* 411, 418.

41 Neither of which includes any fault requirements for liability: *Competition and Consumer Act 2010* (Cth) sch 2.

This approach is preferable to the establishment of an entirely separate legislative framework,[42] or to leaving these issues open and therefore uncertain in key respects.

Abolition of common law actions

4.38 The Terms of Reference ask whether, in the event that the statutory action is enacted, any common law actions should be abolished. Such a provision may be unnecessary, depending on common law developments at the time of enactment. However, such a provision would create certainty.

4.39 There is no case for abolishing the equitable action for breach of confidence in its entirety, as it protects 'confidential' information whether or not it is also private in nature.

4.40 The NSWLRC recommended the enactment of the following provision:

> To the extent that the general law recognises a specific tort for the invasion or violation of a person's privacy, that tort is abolished.[43]

4.41 To capture possible tort and equitable developments at common law, the Act might provide that to the extent that the general law recognises a specific cause of action for the invasion of a person's privacy, that cause of action is abolished.

Overview of the elements of the new tort

4.42 In the following chapters, the ALRC proposes the elements of a new tort for serious invasion of privacy. There are five elements, and each of them must be satisfied for the plaintiff to have a cause of action. There are significant interactions between the elements, and the ALRC's reasons for proposing the content of one proposal will often depend on the proposals for the other elements. It is therefore important to consider these elements together.

First element: The invasion of privacy must occur by:

(a) intrusion into the plaintiff's seclusion or private affairs (including by unlawful surveillance); or

(b) misuse or disclosure of private information about the plaintiff.

Second element: The invasion of privacy must be either intentional or reckless.

Third element: A person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances.

---

42 This is the approach in, for example, the Australian Consumer Law, in respect of liability for misleading or deceptive conduct.

43 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWLRC Draft Bill, cl 80(1).

Fourth element: The court must consider that the invasion of privacy was 'serious', in all the circumstances, having regard to, among other things, whether the invasion was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff.

Fifth element: The court must be satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest in the defendant's conduct.

5. Two Types of Invasion and Fault

Contents

Summary

5.1 In this chapter, the ALRC proposes two of the five elements of a new tort for serious invasion of privacy.

5.2 Firstly, the ALRC proposes that the new tort be confined to two types of invasion of privacy. The plaintiff must prove that the invasion of privacy occurred either by:

(a) intrusion into the plaintiff's seclusion or private affairs (including by unlawful surveillance); or

(b) misuse or disclosure of private information about the plaintiff.

5.3 These two types of invasion of privacy are widely considered to be the core of a right to privacy—and the chief mischief that needs to be addressed by a new action. Confining the tort to these two types of invasion of privacy will also make the scope of the tort more certain and predictable.

5.4 Secondly, this chapter considers the fault element of the new tort. The ALRC proposes that, for an action under the tort to succeed, the invasion of privacy must be either intentional or reckless. These fault elements are common to existing torts of trespass, such as assault and battery. The ALRC considers that other possible fault elements (such as negligence or strict liability) may make the scope of the new tort too broad.

A cause of action for two types of invasion of privacy

Proposal 5–1 **First element of action:** The new tort should be confined to invasions of privacy by:

(a) intrusion upon the plaintiff's seclusion or private affairs (including by unlawful surveillance); or

(b) misuse or disclosure of private information about the plaintiff (whether true or not).

5.5 Misuse of private information and intrusion upon seclusion have been said to lie at the heart of any legal protection of privacy. Unwanted access to private information and unwanted access to one's body or personal space have been called the 'two core components of the right to privacy'.[1] Most examples of invasions of privacy given to support the introduction of a new cause of action, and most cases in other jurisdictions relating to invasions of privacy, fall into one of these two categories. To provide clarity, certainty and guidance about the purpose and scope of the new action, the ALRC proposes that the action be explicitly confined to these two types of invasion of privacy.[2] This means that invasions of privacy that do not fall into one of these two categories will not be actionable under the new tort.[3]

5.6 Although, as discussed below, many stakeholders said the Act should contain a non-exhaustive list of examples of conduct which may be an invasion of privacy, others noted the benefits of confining the action. Telstra submitted that a non-exhaustive list of examples would allow for the possibility of other types of invasion of privacy to be actionable, and that this would give rise to undesirable uncertainty:

> Categories of conduct caught by any cause of action should be listed exhaustively, using unambiguous and objective terms, in order to reduce the uncertainty and impact that the introduction of such a cause of action would cause to businesses and service providers.[4]

5.7 The two categories of invasion of privacy proposed above draw on the well-known categorisation of privacy torts in the United States, first set out by William Prosser in 1960, and followed in the US *Restatement of the Law Second, Torts*.[5] Prosser wrote that the law of privacy

> comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in

---

1 M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [2.07], cited with approval in *Goodwin v NGN* [2011] EWHC 1437 (QB) (09 June 2011) [85].

2 This is similar to the approach recommended by the VLRC. As discussed further below, the VLRC recommended two separate causes of action, though with very similar elements: one for intrusion upon seclusion and the other for misuse of private information.

3 As discussed below, such conduct may be actionable under other causes of action, such as defamation.

4 Telstra, *Submission 45*.

5 American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652A. Professor Prosser was one of the reporters.

> common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone'. Without any attempt to exact definition, these four torts may be described as follows:
>
> 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> 2. Public disclosure of embarrassing private facts about the plaintiff.
>
> 3. Publicity which places the plaintiff in a false light in the public eye.
>
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[6]

5.8 The ALRC considers that, in Australia, a new privacy tort should be confined to the first two of these four categories. In *ABC v Lenah Game Meats Pty Ltd*, Gummow and Hayne JJ said that 'the disclosure of private facts and unreasonable intrusion upon seclusion, perhaps come closest to reflecting a concern for privacy "as a legal principle drawn from the fundamental value of personal autonomy"'.[7] These two types of invasion of privacy are discussed further below.

Intrusion upon seclusion or private affairs

5.9 Intrusion upon seclusion is one of the two most commonly recognised categories of invasion of privacy. The ALRC considers it essential that the new tort capture this type of conduct.

5.10 The tort of intrusion upon seclusion, Prosser wrote in 1960, 'has been useful chiefly to fill in the gaps left by trespass, nuisance, the intentional infliction of mental distress, and whatever remedies there may be for the invasion of constitutional rights'.[8] These gaps remain in Australian protection of privacy from intrusion today.

5.11 Prosser cited a number of US cases involving intrusion upon seclusion, including cases in which the defendant intruded into someone's home, hotel room and 'stateroom on a steamboat', and upon a woman in childbirth. The principle was 'soon carried beyond such physical intrusion' and 'extended to eavesdropping upon private conversations by means of wire tapping and microphones' and to 'peering into the windows of a home'.[9] Prosser cited a case in which a creditor 'hounded the debtor for a considerable length of time with telephone calls at his home and his place of employment' and another case of 'unauthorized prying into the plaintiff's bank account'.[10]

---

6 William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389.

7 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 251 (Gummow and Hayne JJ), quoting Sedley LJ in *Douglas v Hello!* [2001] 2 WLR 992, 1025.

8 Prosser, above n 6, 392.

9 Ibid 389–92; *Jones v Tsige* (2012) 108 OR (3rd) 241.

10 Prosser, above n 6, 389–92.

5.12 Section 652B of the US *Restatement of the Law Second, Torts* concerns intrusion upon seclusion, and states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

5.13 The accompanying commentary in the *Restatement* reads:

> a. The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.
>
> b. The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.[11]

5.14 The US tort of intrusion has been said to focus on 'the means of obtaining private information rather than on the publication of the information so gained. The core of the tort is the offensive prying into the private domain of another'.[12]

5.15 In the United Kingdom, there is no comparable tort for invasions of privacy by intrusion upon seclusion, falling short of trespass and nuisance.[13] The House of Lords in *Wainwright v Home Office*[14] 'expressly declined to recognize a general right to privacy which would extend to physical privacy interferences not involving the dissemination of information'.[15]

5.16 This apparent gap in the UK law may not be so concerning as it is in Australia, because the UK has a *Protection from Harassment Act 1997* (UK), which provides some legislative protection against invasions of privacy by intrusion into seclusion. In Chapter 14, the ALRC proposes the introduction of a statutory cause of action for harassment, in the event that the proposed privacy tort is not introduced.

---

11 American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652B.
12 Warby et al, above n 1, [3.68].
13 'Unlike US law, there is, as yet, no general tort of intrusion recognised by English law': Raymond Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) 186.
14 *Wainwright v Home Office* [2004] 2 AC 406.
15 Warby et al, above n 1, [10.04].

5.17 Although there is no tort for intrusion upon seclusion in the UK, courts have recognised the potential for intrusions to invade privacy and cause harm. The majority of the House of Lords in *Campbell v MGN Ltd* emphasised that the covert way in which private information about the model Naomi Campbell, later published, was obtained in that case, heightened the invasion of Campbell's privacy. Lord Hoffman said: 'the publication of a photograph taken by intrusion into a private place (for example, by a long distance lens) may in itself be such an infringement [of the privacy of the personal information], even if there is nothing embarrassing about the picture itself'.[16] Similarly, in *Murray v Express Newspapers,* Sir Anthony Clarke MR said that, '"the nature and purpose of the intrusion" is one of the factors which will determine whether the claimant had a reasonable expectation of privacy'.[17]

5.18 Further, in a number of recent cases, the English and European courts have begun to emphasise the intrusive aspects of the conduct under consideration, not only in the way the private information was collected,[18] but also in the effect the publication will have on the claimant's and related parties' lives after publication.[19] Intrusive behaviour by the UK media led to the Leveson Inquiry into the Culture, Practice and Ethics of the Press.[20]

5.19 Discussing the 'curious' resistance of the English courts to recognise a cause of action for intrusion, Raymond Wacks writes that nevertheless

> there are a number of *obiter dicta* that imply that the clandestine recordings of private matters does 'engage' Article 8, that the mere taking of a photograph of a child or an adult in a public place might fall within the category of 'misuse'. These pronouncements are either (uncharacteristic) judicial lapses or subtle, possibly even subconscious, acknowledgements of the present anomaly![21]

5.20 It remains to be seen whether a separate cause of action for intrusion upon seclusion will be recognised at common law in the UK.[22] The authors of *Gurry on Breach of Confidence* note that the case for recognising a separate *tort* of privacy, as opposed to an extended equitable action for disclosure of private information, will be stronger if the courts seek to protect against intrusions into private life as well.[23]

5.21 A New Zealand court has recognised a tort of intrusion upon seclusion, in a case about a man who installed a recording device in a bathroom and recorded his female flatmate showering. In this case, *C v Holland*, Whata J said that the 'critical issue I must determine is whether an invasion of privacy of this type, without publicity or the

---

16 *Campbell v MGN Ltd* [2004] 2 AC 457, [75].

17 *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [36]. See also Warby et al, above n 1, [10.06].

18 See further NA Moreham, 'Beyond Information: The Protection of Physical Privacy in English Law' (2014) 73(2) *Cambridge Law Journal* (forthcoming). See also, *Tsinguiz v Imerman* [2010] EWCA Civ 908 [66] in which it was held that misuse of confidential information for the equitable cause of action may include intentional observation and acquisition of the information.

19 *Goodwin v News Group Newspapers Ltd* [2011] EWHC 1437 (QB); *Mosley v United Kingdom – 48009/08* [2011] ECHR 774; *A v United Kingdom – 35373/97* [2002] ECHR 811; [2003] EHRR 51.

20 See further *The Leveson Inquiry* <www.levesoninquiry.org.uk>.

21 Wacks, above n 13, 247 (citations omitted).

22 See further Moreham, above n 18.

23 Tanya Aplin et al, *Gurry on Breach of Confidence* (Oxford University Press, 2nd ed, 2012) [7.102].

prospect of publicity, is an actionable tort in New Zealand'.[24] The court concluded that it was:

> the similarity to the *Hosking* tort [discussed below] is sufficiently proximate to enable an intrusion tort to be seen as a logical extension or adjunct to it. This Court can apply, develop and modify the tort to meet the exigencies of the time.[25]

5.22 In defining the ingredients of the tort, Whata J drew guidance from the decision of the Ontario Court of Appeal in *Jones v Tsige*,[26] which had recognised a tort of intrusion into seclusion. Whata J stated:

> I consider that the most appropriate course is to maintain as much consistency as possible with the North American tort given the guidance afforded from existing authority. I also consider that the content of the tort must be consistent with domestic privacy law and principles. On that basis, in order to establish a claim based on the tort of intrusion upon seclusion a plaintiff must show:
>
> (a) An intentional and unauthorised intrusion;
>
> (b) Into seclusion (namely intimate personal activity, space or affairs);
>
> (c) Involving infringement of a reasonable expectation of privacy;
>
> (d) That is highly offensive to a reasonable person.[27]

5.23 Including intrusion as one of the categories of an actionable invasion of privacy in the new statutory action would remedy one of the key deficiencies in the Australian protection of privacy law identified in Chapter 3. It would enable people to take steps to prevent unjustifiable conduct or obtain some redress where they have been the target of deliberate and unjustifiable intrusions but where, often for historical or technical reasons, the circumstances do not fall within the protection of existing tort and other laws.

Misuse or disclosure of private information

5.24 The second type of invasion of privacy that the ALRC proposes should be covered by the new privacy tort is misuse or disclosure of private information about the plaintiff. It will be neither surprising nor contentious that a cause of action for invasion of privacy will in part concern the disclosure of private information. Lord Hoffmann has identified 'the right to control the dissemination of information about one's private life' as central to a person's privacy and autonomy.[28]

5.25 This is a widely recognised type of invasion of privacy, already actionable in the UK, the US, New Zealand, Canada and elsewhere. Most cases involving private information are concerned with unauthorised disclosure.

---

24 *C v Holland* [2012] 3 NZLR 672 (24 August 2012) [1].

25 Ibid [86].

26 *Jones v Tsige* (2012) 108 OR (3rd) 241. There the defendant, who was in a relationship with the claimant's former husband, and who worked for the same bank as the claimant in different branches, used her workplace computer to gain access to the claimant's private banking records 174 times. Again there was no publication.

27 *C v Holland* [2012] 3 NZLR 672 (24 August 2012) [94]–[95] (Whata J).

28 *Campbell v MGN Ltd* [2004] 2 AC 457, [51].

5.26 The elements of the US tort, set out in the *Restatement of the Law Second, Torts*, are that publicity is given to a matter concerning the private life of another, and 'the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public'.[29] Publicity, the commentary to the *Restatement* says, 'means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge'.[30]

5.27 The disclosure of private information is now also a settled basis for action in the UK. The new or extended cause of action has developed out of the equitable cause of action for breach of confidence, as formulated in *Campbell v MGN Ltd*, since the enactment of the *Human Rights Act 1998* (UK), which incorporates elements of the *European Convention on Human Rights* (ECHR).[31] Article 8 of the ECHR provides, in part, that 'everyone has the right to respect for his private and family life, his home and his correspondence'. Although Article 8 is not confined to private information, the focus of the UK action on disclosure of private information may be partly attributed to its roots in the equitable doctrine of breach of confidence, which protects confidential information.

5.28 The New Zealand courts have recognised a new tort of invasion of privacy by giving publicity to private facts. Gault P and Blanchard J stated in *Hosking v Runting*:

> The elements of the tort as it relates to publicising private information set down by Nicholson J in *P v D* provide a starting point, and are a logical development of the attributes identified in the United States jurisprudence and adverted to in judgments in the British cases. In this jurisdiction it can be said that there are two fundamental requirements for a successful claim for interference with privacy:
>
> 1. The existence of facts in respect of which there is a reasonable expectation of privacy; and
>
> 2. Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.[32]

Whether true or not

5.29 The ALRC proposes that the new Australian tort refer to private 'information', rather than 'facts'. The use of the word 'fact' in this statutory tort may imply that the relevant private information must be true, for it to be the subject of the cause of action. The ALRC considers that a person's privacy can be invaded by the disclosure of untrue information, if it would be an invasion of privacy if the information were true.

---

29 American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652D.

30 Ibid (commentary on § 652D).

31 *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).

32 *Hosking v Runting* (2005) 1 NZLR 1, [117].

5.30 This is consistent with the *Privacy Act 1988* (Cth), in which personal information is defined in section 6 to include information or an opinion 'whether true or not'.[33] It is also the position in UK law, and is supported by the ALRC. Former judge of the UK High Court, David Eady has written that

> a claimant is not now expected to go through an article about (say) his or her sex life, or state of health, in order to reveal that some aspects are true and others false. That would defeat the object of the exercise and involve even greater intrusion. Any speculation or factual assertions on private matters, whether true or false, can give rise to a cause of action.[34]

5.31 This should be made clear in the new Act by adding the words 'whether true or not' after 'misuse or disclosure of private information about the plaintiff', as proposed above.

5.32 For the plaintiff to have an action, the untrue information must of course also be matters about which the plaintiff has a reasonable expectation of privacy and, as proposed below, the misuse or disclosure must be serious. This is not a proposal for an action for the publication of untrue information.

Misuse or disclosure

5.33 Daniel Solove has argued that privacy 'involves more than avoiding disclosure; it also involves the individual's ability to ensure that personal information is used for the purposes she desires'.[35]

5.34 Disclosure of personal information is perhaps the most common type of misuse of personal information that will invade a person's privacy. Wacks writes that the 'tort of misuse of private information obviously requires evidence of *misuse* which, in practice, signifies *publication* of such information'.[36]

5.35 It is important to note that many invasions of privacy that seem to involve misuse, but not publication, of private information, may better be considered intrusions into private affairs. For example, an employee of a company who, without authorisation, accesses private information of a customer may have intruded into the private affairs of that customer. Such an intrusion would be covered by the first category of invasion proposed by the ALRC. Nevertheless, the ALRC considers that it is reasonable not to confine this second type of invasion to disclosure as some other type of misuse of private information may invade a person's privacy.

Public disclosure

5.36 The ALRC proposes that a disclosure of private information need not be public, in the sense of wide publicity, to satisfy this element of the cause of action. The fact

---

33 *Privacy Act 1988* (Cth).

34 David Eady, 'Injunctions and the Protection of Privacy' (2010) 29 *Civil Justice Quarterly* 411, 422: 'It soon became established in *McKennitt v Ash* [2006] and in *Browne v Associated Newspapers Ltd* [2007], also in the Court of Appeal, that a remedy will lie in respect of intrusive information irrespective of whether it happens to be true or false'.

35 Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1108.

36 Wacks, above n 13, 247, paraphrasing Lord Hoffmann in *Campbell v MGN Ltd* [2004] 2 AC 457, [51].

that the disclosure of personal information was to only one other person should not, in some circumstances, prevent the conduct being held to be actionable, if the circumstances are adjudged to be serious.

5.37 The US tort, on the other hand, is confined to public disclosures. The *Restatement of the Law Second, Torts*, states that publicity means 'the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge'.[37]

5.38 The New Zealand Court of Appeal seemed also to have in mind public disclosures when discussing the tort, in *Hosking v Runting*. In that case, Gault P and Blanchard J said: 'I see no reason why our courts should not develop the action for breach of confidence to protect personal privacy through the public disclosure of private information where it is warranted'.[38]

5.39 However, the ALRC proposes not to confine the action to public disclosures. The fact that a disclosure of personal information was not public may make it more difficult for a plaintiff to satisfy other elements of the action. For example, it may suggest the invasion of privacy was less serious than it might otherwise have been. Also, the plaintiff's expectation of privacy may not always extend to non-public disclosures of personal information. However, there may be some instances in which a plaintiff does have a reasonable expectation not to have personal information disclosed even within a small circle, and the disclosure will be adjudged serious.[39]

False light and appropriation

5.40 The ALRC considers that the third and fourth torts identified by Prosser should not be included in a new Australian tort for serious invasion of privacy. Discussing the four US torts, the Australian High Court has said that, in Australia, one or more of the four types of invasion of privacy would often 'be actionable at general law under recognised causes of action':

> Injurious falsehood, defamation (particularly in those jurisdictions where, by statute, truth of itself is not a complete defence), confidential information and trade secrets (in particular, as extended to information respecting the personal affairs and private life of the plaintiff, and the activities of eavesdroppers and the like), passing-off (as extended to include false representations of sponsorship or endorsement), the tort of conspiracy, the intentional infliction of harm to the individual based in *Wilkinson v Downton* and what may be a developing tort of harassment, and the action on the case for nuisance constituted by watching or besetting the plaintiff's premises, come to mind.[40]

5.41 The disclosure of private facts and unreasonable intrusion upon seclusion concern the key privacy interests, such as personal dignity and autonomy, whereas the

---

37 American Law Institute, *Restatement of the Law Second, Torts* (1977).

38 *Hosking v Runting* (2005) 1 NZLR 1.

39 See, for example, *Giller v Procopets* (2008) 24 VR 1.

40 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255 (Gummow and Hayne JJ).

other US torts arguably protect others' interests. Gummow and Hayne JJ stated in *ABC v Lenah Game Meats*:

> Whilst objection possibly may be taken on non-commercial grounds to the appropriation of the plaintiff's name or likeness, the plaintiff's complaint is likely to be that the defendant has taken the steps complained of for a commercial gain, thereby depriving the plaintiff of the opportunity of commercial exploitation of that name or likeness for the benefit of the plaintiff. To place the plaintiff in a false light may be objectionable because it lowers the reputation of the plaintiff or causes financial loss or both.[41]

5.42 Wacks has written that the 'false light' category 'seems to be both redundant (for almost all such cases might equally have been brought for defamation) and only tenuously related to the protection of the plaintiff against aspects of his or her private life being exposed'.[42] The ALRC has proposed some protection, if the falsity relates to matters as to which the plaintiff has a reasonable expectation of privacy.

5.43 Professor Michael Tilbury has written that, for the most part, the interests protected by the US torts of appropriation of the plaintiff's name or likeness and false light, 'can or ought to be restated as, respectively, the commercial interest (or property) that plaintiffs have in their identity and the interest that plaintiffs have in their reputation'.[43] However, although privacy may have a wider reach, at the 'heart of privacy law', Tilbury writes, are the torts of public disclosure of private facts and intrusion on seclusion.[44]

5.44 As Gummow and Hayne JJ foreshadowed, there could be some objection taken to appropriation of image or name on non-commercial grounds, thus outside the law of passing off and the like, and this risk has been heightened in the digital era. The ALRC considers that the two categories set out in the proposal should be sufficient to protect the privacy of the individual. Any further reform to the law relating to image rights would need to be considered in the context of Australia's existing intellectual property law.

Examples of invasions of privacy

5.45 Confining the new tort to these two broad and widely recognised categories of invasion of privacy is preferable to two other options that have been considered. The first option is to provide no statutory guidance on the meaning of invasion of privacy, and to leave this to be developed by the courts. A second option would be to include examples of invasion of privacy.

5.46 The ALRC considers that the new Act should provide as much certainty as possible on what may amount to an invasion of privacy. This will make the scope of the action more predictable, particularly as privacy itself is not defined in the new Act.

---

41 Ibid, 256 (Gummow and Hayne JJ).
42 Wacks, above n 13, 181.
43 Michael Tilbury, 'Coherence, Non-Pecuniary Loss and the Construction of Privacy' in Jeffrey Berryman and Rick Bigwood (eds), *The Law of Remedies: New Directions in the Common Law* (Irwin Law, 2010) 127, 136.
44 Ibid 137.

As discussed above, the ALRC proposes that some certainty be provided by having the new Act describe, in general terms, the two categories of invasion of privacy to which the action would be confined.

5.47 However, another way to provide guidance might be to include in the new Act broad examples of invasions of privacy. This approach would make the cause of action more flexible, but at the cost of certainty. This was the approach favoured by the ALRC in its 2008 report, in which it recommended that the relevant Act contain the following non-exhaustive list of types of invasion that fall within the cause of action:

- 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.[45]

5.48 A number of stakeholders in the current Inquiry said a non-exhaustive list of examples should be included in the new provision,[46] stressing that this would provide courts, parties and business with some guidance and certainty.[47] Some of these stakeholders may prefer the greater certainty that confining the action in the way the ALRC proposes will provide. Some stakeholders said the examples should be general and flexible, so that that the action can 'evolve with social and technological developments'.[48]

5.49 Jansz-Richardson said the examples should be 'relatively general in nature to ensure their ability to translate over time'.[49] Public Interest Advocacy Centre (PIAC) submitted that examples should be 'open-ended and inclusive, which would build sufficient flexibility into the proposed cause of action for it to be appropriately adapted to changing social and technological circumstances'.[50] The Australian Privacy Foundation said 'the list should be clearly identified as non-exclusive and non-exhaustive, ie courts should be able to deal with serious invasions of privacy that fall outside the list'.[51]

---

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

46 Office of the Australian Information Commissioner, *Submission 66*; NSW Young Lawyers, *Submission 58*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Telstra, *Submission 45*; Electronic Frontiers Australia, *Submission 44*; Optus, *Submission 41*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; C Jansz-Richardson, *Submission 24*; Office of the Information Commissioner, Queensland, *Submission 20*; Insurance Council of Australia, *Submission 15*.

47 Telstra, *Submission 45*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; Insurance Council of Australia, *Submission 15*. Examples 'may be useful in guiding courts and more broadly in addressing unfounded anxieties about the purpose of the legislation or its scope': Australian Privacy Foundation, *Submission 39*. A 'list of examples should be included in the Act to provide guidance to business': Telstra, *Submission 45*.

48 Office of the Australian Information Commissioner, *Submission 66*.

49 C Jansz-Richardson, *Submission 24*.

50 Public Interest Advocacy Centre, *Submission 30*.

51 Australian Privacy Foundation, *Submission 39*.

5.50 Other stakeholders said that the cause of action should not include a list of examples.[52] Some were concerned the list would narrow the scope of the action, by implying that invasions of privacy not covered by an example would not be actionable.[53] It was also suggested that the examples in the list might become outdated.[54] Other stakeholders suggested that examples were unhelpful because privacy was 'contextual and depends on facts and circumstances'.[55] The ABC said there needs to be 'an intense focus on how the various interests at stake are implicated in the particular circumstances of each case'.[56] SBS submitted that 'the key for any statutory cause of action is flexibility':

> The more activities or matters that are included to 'assist' with the formulation of a breach of privacy action, the more likely it is that these tests will become rigid and inflexible. It is vital that courts consider each case on its facts.[57]

5.51 Some stakeholders suggested that more specific examples of invasion of privacy might be included in the Act. For example, Electronic Frontiers Australia submitted that there should be examples for data breaches, aggregated collections of data, and 'posting of photographs, audio-recordings, and video-recordings of personal spaces, activities, and bodies for which consent to post has not been expressly provided by the participant'.[58]

5.52 However, the ALRC considers that the application of the tort to more specific and particular circumstances is best left to the courts to consider on a case by case basis, but within the confines of the two categories specified. Specific examples may provide additional guidance, but they also carry a greater risk of distracting the court from the consideration of the distinct facts and circumstances of a particular case.

One cause of action, not two

5.53 The ALRC proposes that there be one cause of action covering the two broad types of invasion of privacy. A similar approach, recommended by the Victorian Law Reform Commission (VLRC), would be to enact two separate but 'overlapping' causes of action. However, enacting separate causes of action should only be necessary if the elements of each would be substantially different, which the ALRC considers is not the case. Separate actions should therefore not be necessary.

---

52 SBS, *Submission 59*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*; Law Institute of Victoria, *Submission 22*; Pirate Party of Australia, *Submission 18*; P Wragg, *Submission 4*.

53 P Wragg, *Submission 4*; Law Institute of Victoria, *Submission 22*. Wragg submitted that this 'may be harmful to the longevity of the act to be too specific on the scope of its ambit since it may be read narrowly in order to prevent application to novel and unexpected technological developments as they arise.' The Law Institute of Victoria submitted that this 'might give would-be defendants the impression that conduct outside the parameters of the list does not constitute an invasion of privacy'.

54 Law Institute of Victoria, *Submission 22*. For example, the Law Institute of Victoria stated that: 'In the current technological age, it is likely that any examples in a list could be quickly superseded by other types of privacy invasions that might evolve in the future'.

55 Ibid.

56 ABC, *Submission 46*.

57 SBS, *Submission 59*.

58 Electronic Frontiers Australia, *Submission 44*.

5.54 The VLRC's reasons for recommending two causes of action largely relate to the widely recognised difficulty of defining privacy:

> Legislating to protect these broadly recognised sub-categories of privacy is likely to promote greater clarity about the precise nature of the legal rights and obligations that have been created than by creating a broad civilly enforceable right to privacy.[59]

5.55 The ALRC has come to a similar conclusion, which is one reason it proposes that the action be confined to two more precisely defined sub-categories of invasion of privacy. The categories proposed by the ALRC are broadly the same as the categories identified by the VLRC.

5.56 Although the ALRC and VLRC approaches are broadly consistent, the ALRC considers it important that there be only one cause of action. The availability of two causes of actions may cause unnecessary overlap and duplication in many cases in which both types of invasion arise. Dr Ian Turnbull submitted that one reason for having only one cause of action is that 'in most cases intrusion upon seclusion will be followed by misuse of the private information obtained by the intrusion'.[60]

5.57 The availability of two torts would increase the length and cost of proceedings and risk duplication in monetary damages. There will already be cases where the cause of action may overlap with other causes of action such as trespass or breach of contract or breach of confidence. It would be undesirable to risk inviting further duplication.

5.58 Many stakeholders favoured a single cause of action,[61] however, often because this was thought to make the action more flexible—that is, open to invasions other than by misuse of personal information or intrusion upon seclusion. Dr Normann Witzleb for example said the action should be formulated broadly, to leave its further development to the courts.[62] The Australian Privacy Foundation likewise said that introducing two torts may result in some privacy breaches not being covered.[63] However, the ALRC proposes that the new tort should not be broadly drafted to capture all invasions of privacy, but rather should be confined to the two more precisely defined types of invasion of privacy that are the key mischief that the cause of action is designed to remedy.

Fault—intentional or reckless

Proposal 5–2 Second element of action: The new tort should be confined to intentional or reckless invasions of privacy. It should not extend to negligent invasions of privacy, and should not attract strict liability.

---

59 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) [7.126].

60 I Turnbull, *Submission 5*.

61 Office of the Australian Information Commissioner, *Submission 66*; SBS, *Submission 59*; Electronic Frontiers Australia, *Submission 44*; Optus, *Submission 41*; Australian Privacy Foundation, *Submission 39*; N Witzleb, *Submission 29*; Law Institute of Victoria, *Submission 22*.

62 N Witzleb, *Submission 29*.

63 Australian Privacy Foundation, *Submission 39*.

5.59 The ALRC proposes that the cause of action be confined to intentional or reckless invasions of privacy, even though this will mean that a person whose privacy has been invaded may in some cases have no remedy under the new tort. If the new tort attracted strict liability, or extended to negligent invasions of privacy, this might expose a wide range of people to liability for common human errors. It might also inhibit expression in those who fear incurring liability for unintentionally invading someone's privacy.

5.60 Fault is a key element in any cause of action leading to personal liability to pay compensation for loss or damage caused to another person. Legislating to protect these broadly recognised sub-categories of privacy is likely to promote greater clarity about the precise nature of the legal rights and obligations that have been created than by creating a broad enforceable right to privacy.

5.61 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.

5.62 There are essentially three types of fault to consider when designing a statutory cause of action for serious invasion of privacy:

- **Intentional or reckless:** The defendant must be shown to have intended to invade the privacy of the plaintiff. Intent may also be inferred if the defendant's actions were reckless.[64]
- **Negligent**: Negligence depends on whether the actor's conduct measured up to an objective standard of what a reasonable person in the position of the defendant would or would not do in the circumstances. This is an objective test, in which the intentions of the defendant are not relevant.[65]
- **Strict liability**: If the cause of action is one of strict liability, then the defendant may be liable even though the defendant's actions were not intentional, reckless or negligent.

5.63 Strict liability is 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

64 *Wilkinson v Downton* (1897) 2 QB 57; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417, [80] (Spigelman CJ).

65 *Blyth v Birmingham Waterworks Company* (1856) 11 Ex Ch 781; *Vaughan v Menlove* (1837) 132 ER 490 (CP).

> infliction of harm. That is not a statement of law but a description of the general trend.[66]

5.64 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. It is the fact of defamation, not the intention of the defendant, that generates liability. *Fleming's The Law of Torts* states that the

> justification for this stringent liability is presumably that it is more equitable to protect the innocent defamed rather than the innocent defamer (who, after all, chose to publish); another is that the publication, not the composition of the libel, is the actionable wrong, making the state of mind of the publisher, not the writer, relevant. On the other hand, since one does not as a rule act at one's peril, why should the law demand that one publish at one's peril, especially when what one says is not defamatory on its face? Does reputation deserve a higher level of protection than personal safety?[67]

5.65 However, the uniform *Defamation Acts* that came into force in the Australian states and territories in 2006 provide for a defence of innocent dissemination,[68] which makes liability for defamation somewhat less strict. This defence is available where the defendant proves, among other things, that he or she 'neither knew, nor ought reasonably to have known, that the matter was defamatory'.[69]

5.66 Another example is the action in tort 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 and territory Fair Trading Acts;[70]
- statutory liabilities for damage caused by defective products;[71] and
- statutory liability for damage caused by aircraft.[72]

5.67 Previous law reform reports have diverged on the issue of fault. In 2008, 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

---

66 *Northern Territory v Mengel* (1995) 185 CLR 307, [341]-[342] (Mason CJ, Dawson, Toohey, Gaudron and McHugh JJ).

67 C Sappideen and P Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) 630.

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

69 Ibid s 32(1)(b).

70 *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, for example, *Fair Trading Act 1987* (NSW) s 28.

71 *Competition and Consumer Act 2010* (Cth) sch 2, ss 138-141.

72 See, for example, *Damage by Aircraft Act 1999* (Cth) s 10.

the *Criminal Code* (Cth).[73] The ALRC said that 'including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[74]

5.68 Neither the 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*.[75]

5.69 In a New Zealand case about intrusion upon seclusion, *C v Holland*, Whata J said that the plaintiff must show an intentional intrusion, where intentional 'connotes an affirmative act, not an unwitting or simply careless intrusion'.[76]

Negligent invasions

5.70 A number of stakeholders argue that liability for breach of privacy should be imposed either without proof of fault (strict liability), or at least for negligent invasions of privacy, in addition to reckless and intentional invasions of privacy.[77] Some argue that fault should be relevant only to damages, or that reasonable care should be a defence.[78]

5.71 Many stakeholders who called for strict liability or negligence stressed the harm that may be caused by unintentional invasions of privacy.[79] For example, Electronic Frontiers Australia submitted that negligent invasions 'are likely to be as damaging to the affected persons as intentional or reckless invasions, and in many cases may be more damaging'.[80]

5.72 The ALRC points out however, that if actual damage is suffered beyond emotional distress, it may well be the case that the plaintiff would have a tort action in negligence. Whether the defendant owed the plaintiff the necessary legal duty of care would depend on a range of factors, particularly the type of damage suffered by the plaintiff. It is much more straightforward to succeed in a negligence claim where a plaintiff has suffered physical injury or property damage due to another's negligence than where the harm is in the form of psychiatric illness or pure economic loss. However, Australian courts do recognise claims for negligently caused economic loss. Much will depend on whether the defendant knew of the plaintiff and the risk of loss,

---

73 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 2576.

74 ALRC, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) 2577. See also NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 171.

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

76 *C v Holland* [2012] 3 NZLR 672 (24 August 2012) [94]–[95] (Whata J).

77 See, eg, Office of the Australian Information Commissioner, *Submission 66*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; B Arnold, *Submission 28*; T Gardner, *Submission 3*.

78 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.

79 Eg, Women's Legal Services NSW, *Submission 57*; Electronic Frontiers Australia, *Submission 44*; Public Interest Advocacy Centre, *Submission 30*; C Jansz-Richardson, *Submission 24*; Office of the Information Commissioner, Queensland, *Submission 20*. 'In many cases, regardless of the intent of the invasion, the resultant consequences are the same, and the revelation that the circumstances were caused by negligence or a failure to act is likely to be cold comfort to the individual or group whose privacy has been breached': C Jansz-Richardson, *Submission 24*.

80 Electronic Frontiers Australia, *Submission 44*.

whether the defendant had made a representation to the plaintiff and whether the plaintiff was able to protect him or herself from the effects of the defendant's negligence.[81]

5.73 The plaintiff who has suffered as a result of a negligent data breach may also have a claim for breach of contract in which liability will be strict or negligence based, a claim under the Australian Consumer Law or a claim for breach of confidence.

5.74 Some argue that data breaches are often the result of negligence, and if the cause of action included negligence it would encourage companies to take steps to prevent such breaches.[82] Arnold submitted that action for negligence 'provides a necessary and appropriate incentive for Australian organisations to move towards best practice in information management'.[83] PIAC submitted:

> Many systemic breaches of privacy may be due to negligence, rather than to reckless or intentional acts. ... Restricting liability to reckless or intentional acts may also discourage organisations from taking steps to ensure that their privacy management systems are adequate, and may encourage indifference to privacy protection.[84]

5.75 However, under the *Privacy Act* (and to some extent the *Telecommunications Act*) organisations are required to take such steps. Although it could be argued that these Acts have weaknesses, the cause of action should not be designed as a remedy for existing legislation where it would be better for that legislation to be amended or strengthened.

5.76 The Law Institute of Victoria submitted:

> Intentional privacy breaches, such as those alleged against News of the World in the United Kingdom, are not the norm. The larger threat comes from unintentional breaches caused by: a lack of understanding of privacy obligations; technological malfunction and human error; or systemic failures. … Furthermore, requiring intention, rather than negligence, may be difficult to prove against companies.[85]

5.77 If, on the other hand, the new tort were to provide both that the damage for the new tort should include emotional distress and that fault should include negligence, the coherence of the law would be undermined. The proposal would conflict with a clear legislative policy. As outlined above, the primary and most common form of harm suffered from an invasion of privacy is emotional distress. The well-entrenched policy of the common law, reflected in legislation across most Australian states and territories, is that liability for negligence should not extend to emotional distress.[86] If

---

81 *Perre v Apand* (1999) 198 CLR 180.

82 Electronic Frontiers Australia, *Submission 44*: 'Indeed, data breaches … are often the result of negligence. The cause of action should therefore be available for intentional, reckless and negligent invasions of privacy'.

83 B Arnold, *Submission 28*. See also Law Institute of Victoria, *Submission 22*: 'In the absence of a cause of action, there is little to no benefit or incentive for holders of private information in taking privacy obligations seriously'.

84 Public Interest Advocacy Centre, *Submission 30*.

85 Law Institute of Victoria, *Submission 22*.

86 Eg, *Civil Liability Act 2002* (NSW) s 31.

the key type of harm that the new tort aims to avoid or redress is emotional distress, the new tort should be restricted to intentional or reckless conduct.

5.78 Further, entities subject to the *Privacy Act* whose activities result in data breaches, whether caused negligently, accidentally or by systemic problems, will be subject to a range of remedial responses by the Office of the Australian Information Commissioner. From March 2014, this includes the possibility of substantial civil penalties.[87] The ALRC considers that regulatory responses are a better way to deal with data breaches than a civil action for invasion of privacy, but as noted above, in any event many entities may be subject to a range of other civil legal liabilities.

Strict liability

5.79 Some have argued that one reason why liability for invasions of privacy should be strict is that this would be consistent with actions in defamation and breach of confidence.[88] Witzleb has written that the 'majority of torts intended to protect personality interests do not set the bar at reckless or intentional conduct'.[89]

5.80 However, the analogy between these causes of action is imperfect. Breach of confidence arises where there was a pre-existing obligation which informs and binds the defendant's conscience, or knowledge that the information was imparted under that obligation.[90] Defamation is about a narrower range of conduct than the new tort of invasion of privacy and has a wide range of defences including, by statute, the defence of innocent dissemination.

5.81 The OAIC also noted that 'no fault element is required for complaints made to the OAIC for an interference with privacy under the *Privacy Act*. A finding of an interference with privacy can be made in relation to negligent and accidental acts, as well as those which are intentional or reckless'.[91] However, the *Privacy Act* regulates government agencies and corporations which have the resources to take precautions to avoid negligent data breaches; an action under the new tort, on the other hand, could be taken against natural persons, who will usually not have such resources. Further, liability and costs may potentially be greater under the new tort than as a result of the complaints process under the *Privacy Act*. The statutory cause of action potentially applies to a wider range of activities than the *Privacy Act.*

---

87 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

88 'The majority of torts intended to protect personality interests do not set the bar at reckless or intentional conduct. Defamation is a strict liability tort but provides faultless defendants with a defence in some cases ... Likewise, liability under the principles in *Wilkinson v Downton* is now more commonly understood as requiring merely negligence, not intention or recklessness, in relation to the consequence of causing psychiatric harm. Lastly, the proposed Australian Privacy Principles ... impose objective obligations that are akin to a negligence standard, such as conduct must be 'reasonable', 'reasonably necessary', or based on a 'reasonable belief'': Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' (2011) 19 *Torts Law Journal* 104, 118–119.

89 Ibid 118.

90 *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] 1 WLR 1556.

91 Office of the Australian Information Commissioner, *Submission 66*.

Intentional and reckless only

5.82 Other stakeholders, however, argued that the cause of action should be confined to intentional or reckless invasions of privacy.[92] The Australian Bankers Association, for example, submitted, the 'the trend in legislation to more strict liability provisions associated with the imposition of civil penalties continues to be a major concern for the private sector...'

> The cause of action given its likely scope and imprecision should not be cast in the tortious framework of negligence. Rather it should apply only to an intent to seriously interfere with a person's privacy or to do so with reckless indifference to that result and this has occurred.[93]

5.83 Other stakeholders suggested that some invasions of privacy should not attract liability because the conduct is not blameworthy. The Arts Law Centre of Australia submitted the example of a documentary maker 'filming in a public place which looks onto a private apartment where someone is getting undressed' and so accidentally invading someone's privacy.[94] Similarly, SBS submitted:

> There are many ways in which footage, images or other material may breach someone's privacy in a way which is unintentional. A common example would be the kind of footage filmed for use in news broadcasts, often wide angle shots of crowds, or footage of incidental comings and goings out of buildings relevant to a news story. It is very possible that in such a story, a person or incident might be captured that the person considered a breach of their privacy.[95]

5.84 Extending liability to include negligence might lead people to be 'unduly careful about disclosing information'.[96] It may lead to excessive self-censorship or too great a chilling effect on everyday activities that carry even a remote risk of invading privacy.

Intending the act, or intending to invade privacy?

5.85 An intention to invade a person's privacy may be distinguished from an intention to do an act that has the perhaps unintended consequence of invading a person's privacy. In some cases, the consequences of an act will be so inextricably linked to the act, or so substantially certain to follow,[97] that an intention to do the act will strongly suggest an intention to bring about the consequences of the act. But this will not always be the case. Furthermore, it may be quite common to intend an action that will have the consequence of invading someone's privacy, without intending to invade their privacy.

5.86 For example, if an absent-minded person walks into a neighbour's home, thinking it is his or her own home, then the person may have invaded the neighbour's

---

92 SBS, *Submission 59*; Google, *Submission 54*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*; Australian Bankers' Association, *Submission 27*.

93 Australian Bankers' Association, *Submission 27*.

94 Arts Law Centre of Australia, *Submission 43*.

95 SBS, *Submission 59*.

96 Australian Subscription Television and Radio Association, *Submission 47*.

97 Sappideen and Vines, above n 67, 34.

privacy. The action in walking through the front door may have been intended,[98] but the invasion of his neighbour's privacy was not.

5.87 To take a more common example, a media entity may publish a story that in fact invades a person's privacy, but without any knowledge of the facts which would make it an invasion of that person's privacy. The publishing of the story may have been intended, but not the consequences of the publication, namely, the invasion of the person's privacy.

5.88 Some stakeholders said the relevant intent should be an intent to invade the privacy of the plaintiff and not merely an intent to do an act which invades the privacy of the plaintiff.[99] Telstra submitted that, given it considers current privacy protections sufficient, if there were a cause of action,

> intent should be determined by reference to the invasion of privacy and the harm to the complainant, rather than the conduct of the defendant, in order to be as specific and targeted in its application as possible.[100]

5.89 In the ALRC's view, the new tort should only be actionable where the defendant intended to invade the plaintiff's privacy. Some will argue that this will too often remove liability for serious breaches of privacy. However, if it were sufficient merely to intend the act, and not the consequences of the act in the sense of the invasion of privacy, then this would effectively impose a negligence or strict liability standard as in defamation. For reasons discussed above, the ALRC considers that negligence should not be sufficient fault for an action for breach of privacy, and strict liability would be unduly burdensome and discouraging to other worthwhile competing interests.

5.90 If the defendant intended the invasion of privacy, it would not be necessary, in addition, to show that the defendant intended to offend, distress or harm the plaintiff, for the plaintiff to have a cause of action. The question then becomes one of whether or not the particular damage claimed is too remote from the defendant's tort. In intentional torts, the test is whether the damage claimed was a natural and probable consequence of the tort.[101] If the defendant had an intent to inflict harm, this would amount to malice in law and would aggravate the damages that could be claimed. Many invasions of privacy will not be motivated by malice towards the victim. If a media organisation invades a person's privacy, presumably this will be largely motivated by a desire to attract more viewers or increase the sale of newspapers, rather than to harm the victim.

---

98 This would still be a trespass because mistake is no defence to a trespass action: Sappideen and Vines, above n 66, 88.

99 Eg, SBS, *Submission 59*; Telstra, *Submission 45*; Arts Law Centre of Australia, Submission No 15 to DPM&C Issues Paper, 2011.

100 Telstra, *Submission 45*.

101 *Palmer Bruyn & Parker Pty Ltd v Parsons* (2001) 208 CLR 388.

5.91 It would not necessarily be the case that the plaintiff would have to prove that the defendant had a subjective intent to invade his or her privacy. Such an intent may be imputed.[102] If an invasion of privacy is substantially or obviously certain to follow from certain conduct, then the defendant may be taken to have intended the invasion of privacy, even if the defendant in fact did not put his or her mind to invading the plaintiff's privacy. This may also amount to recklessness.[103]

Effect of apology on liability

Proposal 5–3 The new Act should provide that an apology made by or on behalf of a person in connection with any invasion of privacy alleged to have been committed by the person:

(a) does not constitute an express or implied admission of fault or liability by the person in connection with that matter; and

(b) is not relevant to the determination of fault or liability in connection with that matter.

Proposal 5–4 Evidence of an apology made by or on behalf of a person in connection with any conduct by the person should not be admissible in any civil proceedings under the new Act as evidence of the fault or liability of the person in connection with that matter.

5.92 Any apology or correction of published material by a defendant should not be treated in evidence as an admission of fault.[104] This proposal is not intended to limit the operation of the proposals in Chapter 11 on the consideration of mitigating and aggravating factors in a court's assessment of damages.

5.93 This proposal is intended to encourage the early resolution of disputes without recourse to litigation. In many circumstances, an apology that something has occurred may provide a sufficient response to appease someone whose privacy has been invaded and people should feel free to make an apology without it affecting their ultimate or potential liability.

102 *Wilkinson v Downton* (1897) 2 QB 57.

103 *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.

104 This is similar to the following provision: *Civil Liability Act 2002* (NSW) s 69. See also: Prue Vines, 'The Power of Apology: Mercy, Forgiveness or Corrective Justice in the Civil Liability Arena?' (2007) 1 *Public Space* 1; Prue Vines, 'The Apology in Civil Liability: Underused and Undervalued?' (2013) 115 *Precedent* 28; Robyn Carroll, 'Apologies as a Legal Remedy' (2013) 35 *Sydney Law Review* 317; 'Review of the Law of Negligence: Final Report' (2002).

6. A Reasonable Expectation of Privacy

Contents

Summary

6.1 This chapter concerns the third element of the new tort. The ALRC proposes that, to have an action, a plaintiff must prove that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances.

6.2 This is an objective test. The subjective expectation of the plaintiff may be a relevant consideration, but it is not the focus of the inquiry.

6.3 The ALRC also proposes that the new Act include a non-exhaustive list of factors which a court may consider when determining whether a person would have had a reasonable expectation of privacy. This is designed to provide guidance and assistance to the parties and the court.

6.4 The proposed factors include, among other factors, the nature of any information disclosed; the means used to obtain private information or intrude upon the plaintiff's seclusion; whether private information was already in the public domain; and the place where an intrusion occurred.

6.5 Two related issues—the defendant's interest in freedom of expression, and the public interest in the defendant's conduct—are considered together in Chapter 8.

Reasonable expectation of privacy

Proposal 6–1 **Third element of action:** The new tort should only be actionable where a person in the position of the plaintiff would have had a reasonable expectation of privacy, in all of the circumstances.

6.6 Whether a plaintiff has a reasonable expectation of privacy is a useful and widely adopted test of what is private, for the purpose of a civil cause of action for invasions of privacy. The ALRC proposes that, to have an action under the new tort, the plaintiff should be required to establish that a person in the plaintiff's position would have had a reasonable expectation of privacy, in all of the circumstances.

6.7 This is preferable to attempting to define 'privacy' in the Act. It is notoriously difficult to define what is private and the courts have therefore developed a test rather than a definition. In *ABC v Lenah Game Meats*, Gleeson CJ said:

> There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private.[1]

6.8 The use of the 'reasonable expectation' test was supported by a number of stakeholders.[2] It is flexible and adaptable to new circumstances. Matters which an individual or community may reasonably expect will remain private will change between cultures and over time. The Office of the Information Commissioner, Queensland, submitted that the reasonable expectation of privacy test 'would reflect both community standards and provide sufficient flexibility for the modern range of social discourses'.[3]

6.9 Similar tests have been recommended in reports of the ALRC, the NSWLRC and the VLRC.[4] This test is also used in a number of other jurisdictions.[5] It has been adopted in the UK, New Zealand, and several Canadian provinces. In *Campbell v*

---

1 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].

2 Office of the Australian Information Commissioner, *Submission 66*; SBS, *Submission 59*; NSW Young Lawyers, *Submission 58*; Free TV, *Submission 55*; Queensland Council of Civil Liberties, *Submission 51*; Australian Subscription Television and Radio Association, *Submission 47*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Optus, *Submission 41*; Public Interest Advocacy Centre, *Submission 30*; B Arnold, *Submission 28*; C Jansz-Richardson, *Submission 24*; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*; Insurance Council of Australia, *Submission 15*; Women's Legal Centre (ACT & Region) Inc., *Submission 19*; Australian Privacy Foundation, *Submission 39*.

3 Office of the Information Commissioner, Queensland, *Submission 20*.

4 ALRC, *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) 20–26.

5 For example, the UK, Canada, and in New Zealand: 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, 2011) 17–21. In the United Kingdom, Lord Hope in the majority in *Campbell v MGN Ltd* stated that '[t]he 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].

MGM, Lord Nicholls said that 'the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy'.[6]

6.10 The test proposed by the ALRC is an objective test. The court must consider whether it would be reasonable for a person in the position of the defendant to have expected privacy. The subjective expectation of the plaintiff may be a relevant consideration if that has been made manifest, but it is not the focus of the test, nor an essential element that must be satisfied.

6.11 A similar test is used in the US when considering possible violations of Fourth Amendment rights.[7] In *Katz v United States,* Justice Harlan of the US Supreme Court said:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have *exhibited* an actual (subjective) expectation of privacy and, second, that the expectation be one that *society is prepared to recognize as 'reasonable*.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[8]

6.12 Some stakeholders opposed the use of a reasonable expectation test,[9] with some saying that the test was too vague.[10] However, courts are used to determining issues of reasonableness or even reasonable expectation in other contexts.[11] There are notable benefits of using a test that has been used for some time in other jurisdictions: in applying the test, Australian courts will be able to draw on jurisprudence from the UK, New Zealand and the US.

6.13 In *ABC v Lenah Game Meats*, Gleeson CJ proposed a different test for what is private, where the information was not obviously private. He said 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'.[12] Lord Nicholls in *Campbell* said this test should be used with care, for two reasons:

> First, the 'highly offensive' phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the 'highly offensive' formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to

---

6 *Campbell v MGN Ltd* [2004] 2 AC 457, [21].

7 The Fourth Amendment to the *US Constitution* concerns the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'.

8 *Katz v United States* (1967) 389 US 347, 360–361 (emphasis added).

9 Australian Bankers' Association, *Submission 27*; P Wragg, *Submission 4*.

10 Australian Bankers' Association, *Submission 27*.

11 *Rogers v Whitaker* (1992) 175 CLR 479. See also B Arnold, *Submission 28*.

12 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].

> which publication was a matter of proper public concern. This could be a recipe for confusion.[13]

6.14 Baroness Hale also preferred an objective reasonable expectation test, saying that it was 'much simpler and clearer' than an offensiveness test of privacy.[14] Further, Baroness Hale said that it was apparent that Gleeson CJ did not intend for the 'highly offensive' test to be the only test,

> … particularly in respect of information which is obviously private, including information about health, personal relationships or finance. It is also apparent that he was referring to the sensibilities of a reasonable person placed in the situation of the subject of the disclosure rather than to its recipient.[15]

6.15 The ALRC considers that the offensiveness of a disclosure or intrusion may be one matter considered by a court in determining whether there is a reasonable expectation of privacy. However, as proposed further below, 'offence' may also be used to distinguish serious invasions of privacy from non-serious invasions of privacy.

6.16 Although there is a separate element of the tort, proposed further below, that explicitly confines the tort to 'serious' invasions of privacy, the 'reasonable expectation of privacy' test should also help ensure that non-serious privacy interests are not actionable under the tort.

Considerations

Proposal 6–2 The new Act should provide that, in determining whether a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances, the court may consider, among other things:

(a) the nature of the private information, including whether it relates to intimate or family matters, health or medical matters, or financial matters;

(b) the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology;

(c) the place where the intrusion occurred;

(d) the purpose of the misuse, disclosure or intrusion;

(e) how the private information was held or communicated, such as in private correspondence or a personal diary;

(f) whether and to what extent the private information was already in the public domain;

---

13 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
14 Ibid [135].
15 Ibid [136].

(g) the relevant attributes of the plaintiff, including the plaintiff's age and occupation;

(h) whether the plaintiff consented to the conduct of the defendant; and

(i) the extent to which the plaintiff had manifested a desire not to have his or her privacy invaded.

6.17 The ALRC proposes that this non-exhaustive list of considerations should be set out in the Act. It is designed to assist rather than confine the court, when the court assesses whether the plaintiff had a reasonable expectation of privacy. Not all matters can be listed, but the ALRC has listed some of the more common or important matters. Submissions on what matters should be listed are welcome.[16]

6.18 The NSWLRC recommended the inclusion of a comparable list of matters that would help a court determine whether a person's privacy has been invaded.[17]

6.19 In *Murray v Big Pictures*, which concerned photographs taken of a child in the street for commercial publication, the UK Court of Appeal set out a non-exhaustive list of matters a court should consider when determining whether the plaintiff had a reasonable expectation of privacy:

> They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purpose for which the information came into the hands of the publisher.[18]

6.20 Other matters will be relevant in other cases, particularly in cases concerning intrusion upon seclusion. Wacks has suggested that, in an action for intrusion upon seclusion, a court should take into account the following factors when determining whether the claimant had a reasonable expectation of privacy:

(a) the place where the intrusion occurred (for example, whether the claimant is at home, in office premises or in a public place, and whether or not the place is open to public view from a place accessible to the public, or whether or not the conversation is audible to passers-by);

(b) the object and occasion of the intrusion (for example, whether it interferes with the intimate or private life of the claimant); and

---

16 D Butler, *Submission 10*: Professor Butler submitted a list of matters that should be considered. Many of these matters are included in the list proposed by the ALRC, but others include '[i]f a sexual liaison is involved, the intimacy of the sexual relationship'; '[w]hether there is a risk of serious injury to the plaintiff if there is disclosure'; '[w]hether the information is contained in a public record which is part of the public consciousness'; and '[a]ny other circumstances'.

17 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) Draft Bill, cl 74(3)(a).

18 *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [36].

(c) the means of intrusion employed and the nature of any device used (for example, whether the intrusion is effected by means of a high-technology sense-enhancing device, or by mere observation or natural hearing).[19]

Nature of the information

6.21 The nature of the information will often suggest whether or not it is private. Information concerning the plaintiff's intimate or family matters, health or medical matters, and financial matters are all likely to be private.

6.22 Gleeson CJ said in *Lenah* that certain kinds of information about a person may be easy to identify as private, 'such as information relating to health, personal relationships, or finances'.[20]

6.23 'The nature of the subject matter' was included in a list of matters the NSWLRC recommended should be considered in determining whether there has been an invasion of privacy.[21]

6.24 The definition of sensitive information in the *Privacy Act* may also be of assistance to the courts. 'Sensitive information' is defined to mean:

(a) information or an opinion about an individual's:

i) racial or ethnic origin; or

ii) political opinions; or

iii) membership of a political association; or

iv) religious beliefs or affiliations; or

v) philosophical beliefs; or

vi) membership of a professional or trade association; or

vii) membership of a trade union; or

viii) sexual preferences or practices; or

ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.[22]

---

19 Raymond Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) Appendix, Draft Bill, cl 2(2).

20 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].

21 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) Draft Bill, cl 74(3)(a)(i).

22 *Privacy Act 1988* (Cth) s 6.

6.25 In the UK, it has been said, the nature of the information itself 'is plainly of considerable if not prime importance. It may even be decisive in the question of whether the claimant enjoys a reasonable expectation of privacy in respect of it'.[23]

6.26 Intimate matters will often be sexual matters, widely considered to be private. 'There are numerous general statements from English courts to the effect that sexual behaviour is an aspect of private life.'[24]

6.27 However, intimate and family matters can extend beyond sexual matters. Butler submitted that people are 'entitled to expect privacy for anything non-criminal taking place in the home environment, including any conversations or disagreements occurring therein'.[25] Butler also notes that, '[e]ven where the plaintiff has courted publicity, it would normally be expected that his or her family would nevertheless be entitled to their privacy, especially when there are children of a vulnerable age who are involved'.[26]

6.28 Health, medical and financial information is also widely recognised as private.[27]

Means used

6.29 The means used to obtain private information or to intrude upon seclusion will sometimes be relevant to whether or not there is a reasonable expectation of privacy. For example, the fact that the defendant hacked into the plaintiff's personal computer to take personal information, or used a long distance camera lens to peer into the plaintiff's home, may both suggest the plaintiff's privacy has been invaded (regardless of what personal information or photograph is taken). Butler submitted that '[t]he fact that the information could only be obtained through surreptitious means should normally be an indication that in the circumstances there was a high expectation of privacy'.[28]

6.30 Similarly, it may not be reasonable to expect privacy when standing naked at one's front door, in full view of the street. It may however be reasonable to expect privacy in one's bathroom[29] even if a long distance camera lens could, in theory, take a photo through an open window.

---

23 M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [5.28] (citation omitted).

24 Ibid [5.40]. A distinction is sometimes made between the details of a person's sexual life, and the mere fact of a sexual relationship or sexual orientation, with the latter being sometimes considered less private than the former.

25 D Butler, *Submission 10*, citing *McKennitt v Ash* [2005] EWHC 3003 (QB) (21 December 2005) [137]; *Lee v News Group Newspapers Ltd* [2010] NIQB 106 [32], [43]; *Green Corns Ltd v Claverley Group Ltd* [2005] EWHC 958, [53].

26 D Butler, *Submission 10*.

27 Personal information taken from medical records, reports, or interviews are also generally considered private in English courts: Warby et al, above n 23, [5.35].

28 D Butler, *Submission 10*. Butler's submission cited *Shelley Films v R Features* [1994] EMLR 134; *Creation Records Ltd v News Group Newspapers Ltd* (1997) 39 IPR 1.

29 *C v Holland* [2012] 3 NZLR 672 (24 August 2012).

Place of intrusion

6.31 The physical place in which a person's seclusion is intruded upon may have a bearing on whether they had a reasonable expectation of privacy in those circumstances.

6.32 A person will have a greater expectation of privacy in the home than in a public place. More privacy may be expected in a restaurant than when on the street. Privacy may of course be expected in public places in some circumstances,[30] but a person would generally have a lower expectation of privacy when in public.

Purpose of intrusion

6.33 An intrusion into a person's seclusion for a particular purpose may invade that person's privacy, while the same intrusion for a different purpose would not. For example, a patient's reasonable expectation of privacy has not been invaded when a nurse enters the patient's hospital room to take his or her temperature, but may be invaded by a journalist entering the room to take photos of the patient for publication in a newspaper.

6.34 In *Murray v Big Pictures*, the UK Court of Appeal included, in a list of matters a court should consider when determining whether the plaintiff had a reasonable expectation of privacy, 'the nature and purpose of the intrusion' and 'the circumstances in which and the purpose for which the information came into the hands of the publisher'.[31] In that case, the court held that pictures had been

> taken deliberately, in secret and with a view to their subsequent publication. They were taken for the purpose of publication for profit, no doubt in the knowledge that the parents would have objected to them.[32]

6.35 *Tugendhat and Christie's The Law of Privacy and the Media* states, concerning the UK law, that this aspect of the law is 'relatively undeveloped' and it may be 'open to debate how the "purpose of the intrusion" is to be determined (including whether the "purpose" is objective or subjective), and what weight should be accorded to what purposes'.[33]

How information was held or communicated

6.36 This matter relates to the form in which information is held, stored or communicated. Information held in some forms—such as a personal diary—may more clearly suggest that there is a reasonable expectation of privacy with respect to the information than to the same information held in another form.

---

30 It is 'not possible to draw a rigid line between what is private and that which is capable of being witnessed in a public place by other persons': D Butler, *Submission 10*. Butler cited *Andrews v Television New Zealand Ltd* [2009] 1 NZLR 220.

31 *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [36].

32 Ibid [50], quoted in Warby et al, above n 23, [5.124].

33 Warby et al, above n 23, [5.123].

6.37 The authors of *Tugendhat and Christie's The Law of Privacy and the Media* have written that in some cases, 'the principal focus of the court has been on the repository of the information as one likely to contain confidential or private information':

> Personal diaries, private correspondence, together with similarly private written communications, and conversations on the telephone have all been recognized as likely repositories of such information. More recently it has been held that information stored on a personal computer is prima facie confidential.[34]

6.38 New digital technologies will raise other questions. Many emails are treated like private correspondence, but not all information sent by email will be private in nature.

6.39 That a password or some other form of personal identification is required to gain access to a digital location containing personal information should, in the ALRC's view, strongly suggests the information is likely to be subject to a reasonable expectation of privacy.

6.40 Similar reasoning may apply to intrusions upon seclusion. A locked solid door suggests that those in the room behind the door expect complete privacy, but a glass door involves different expectations.

Public domain

6.41 Whether and to what extent the information was in the public domain should be considered when determining if the plaintiff has a reasonable expectation of privacy. In the context of confidential information, the public domain has been said to mean 'no more than that the information in question is so generally accessible that, in all the circumstances, it cannot be regarded as confidential'.[35] It will be seen from this definition that there may be no clear line between what is in the public domain and what is not.

6.42 Private information differs from confidential information in that the former is often private because of its nature, whereas the latter is often confidential only because of the obligation under which it was imparted. Private information will not automatically cease to be private once it is in the public domain. A person's medical records, for example, do not cease to be private when someone wrongly publishes them on a website. Not only will the original publication to the internet be an invasion of privacy, but other subsequent uses of the records may also, in some cases, amount to an invasion of privacy. Eady J said in *McKennitt v Ash*:

> there are grounds for supposing that the protection of the law will not be withdrawn unless and until it is clear that a stage has been reached where there is no longer anything left to be protected. For example, it does not necessarily follow that because personal information has been revealed impermissibly to one set of newspapers, or to readers within one jurisdiction, that there can be no further intrusion upon a claimant's privacy by further revelations. Fresh revelations to different groups of

---

34 Ibid [5.80] (citations omitted).

35 Lord Goff in *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109, 282. Compare *Prince of Wales v Associated Newspapers Ltd* 2007 3 WLR 222.

> people can still cause distress and damage to an individual's emotional or mental well-being.[36]

6.43 However, an expectation of privacy will usually decrease, the more widely a piece of information has been published by someone.

Attributes of the plaintiff

6.44 Some attributes of a plaintiff, such as age, may affect whether the person has a reasonable expectation of privacy. A young person may have an expectation of privacy in some circumstances where an older person does not. Butler submitted that where 'the plaintiff is a child of vulnerable age there would normally be a high expectation that he or she is entitled to a measure of privacy'.[37]

6.45 The occupation of the plaintiff may also be relevant, particularly if the plaintiff is a 'public figure'. Persons in some occupations necessarily or traditionally invite or receive considerable attention from the public. A professional sportsperson or a politician, for example, cannot reasonably expect the same level of privacy as other members of the public, although they can reasonably expect some privacy.

6.46 'The extent to which the individual has a public profile' was included in a list of matters the NSWLRC recommended should be considered in determining whether there has been an invasion of privacy.[38] People who are reluctantly or involuntarily put in the public spotlight, as for example, the victim of a crime or the family of a victim of crime, are a different category to those who seek the limelight.[39]

6.47 The NSWLRC also included in this list the 'extent to which the individual is or was in a position of vulnerability'.[40] Being in a position of vulnerability may not always be an attribute of the plaintiff, but the ALRC agrees that vulnerability may not only make an invasion of privacy more offensive and harmful, but it will sometimes suggest information is private, or that a person should not be intruded upon. A patient in a hospital would seem to have a reasonable expectation of privacy, for instance.[41]

6.48 The culture and background of a plaintiff may also be relevant to whether he or she has a reasonable expectation of privacy. Some information may be considered to be more private in some cultures than in others. These expectations may be well-known in the community.

6.49 For example, the cultural expectations of Aboriginal and Torres Strait Islander peoples and other cultural or ethnic groups may also be relevant in some cases to the reasonable expectation of privacy in the circumstances. The Arts Law Centre of

---

36 *McKennitt v Ash* [2005] EWHC 3003 (QB) (21 December 2005) [81].

37 D Butler, *Submission 10*. Butler cites *Murray v Big Pictures (UK) Ltd* [2009] Ch 481; *Hosking v Runting* (2005) 1 NZLR 1, [147]; *Lee v News Group Newspapers Ltd* [2010] NIQB 106, [44].

38 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) Draft Bill, cl 74(3)(a)(iv).

39 *In re S* [2003] 3 WLR 1425; *Campbell v MGN Ltd* [2004] 2 AC 457, [142].

40 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) Draft Bill cl 74(3)(a)(v).

41 *Kaye v Robertson* [1991] FSR 62.

Australia stressed the importance of considering the 'confidential or culturally sensitive nature of cultural knowledge, stories, images of indigenous Australians'.[42]

Consent

6.50 A plaintiff cannot generally expect privacy where they have freely consented to the conduct that compromises their privacy.[43] Whether or not a plaintiff consented to particular conduct is a matter of fact. Consent may be express or implied. Consent may also be revoked expressly or impliedly.

6.51 Consent is a defence to many torts, including battery and trespass to land, but for a cause of action for serious invasion of privacy, the ALRC considers that consent should be one of a number of factors relevant to the question of whether the plaintiff had a reasonable expectation of privacy.[44]

6.52 There are degrees of consent. A person may consent to disclosing personal information to a small group of people, but not to a large group.[45] Consent may vary in quality and extent: some have questioned whether clicking 'I agree' to a 40,000-word term of a contract is, in fact, consent and there are calls for the whole issue of consent in the context of online services to be reviewed.[46] This is part of a much larger debate which is best discussed in the overall context of consumer protection.

6.53 For the purposes of the new tort, the ALRC considers that the extent and quality of any consent given by the plaintiff will be relevant matters to consider when determining whether the plaintiff had a reasonable expectation of privacy in the circumstances.

Manifested desire for privacy

6.54 The extent to which the plaintiff had manifested a desire not to have his or her privacy invaded should also be a relevant consideration. The author of a document marked 'private' obviously thereby manifests some desire for the document to be treated as private. Similarly, a person who asks to sit in a private room of a restaurant may more reasonably expect privacy than a person who does not.

---

42 Arts Law Centre of Australia, *Submission 43*.

43 'There is one basic principle which can be seen to underlie all the variously named versions of the defence of consent: it is "good sense and justice [that] one who has … assented to an act being done towards him cannot, when he suffers from it, complain of it as a wrong': Warby et al, above n 23, [12.08], quoting *Smith v Baker* [1891] AC 325, 360 (Lord Herschell).

44 In battery, there is 'some debate as to whether the absence of consent is an element of the cause of action that must be established by [the plaintiff], or whether the presence of consent is a defence that must be pleaded and proved by the defendant. The view taken in this chapter is that it is a defence …': K Barker et al, *The Law of Torts in Australia* (Oxford University Press, 2012) 36.

45 In the UK, 'In a publication case, there must be consent to the extent of publication which occurs': Warby et al, above n 23, [12.15]. 'Media publication will be to a wide audience and the defendant will have to show that the claimant consented to the extent of the publication': Ibid [12.07].

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

6.55 Conversely, a court might ask whether the plaintiff had 'courted publicity on the relevant occasion'.[47] A person who has courted publicity cannot expect the same level of privacy as people who have not.

6.56 However, care must be taken here, because it does not follow that such persons forego any right to privacy, just as a person does not, by manifesting a desire for privacy, automatically become entitled to it.

47 D Butler, *Submission 10*. Butler cites *Hickey v Sunday Newspapers Ltd* [2010] IEHC 349.

7. Seriousness and Proof of Damage

Contents

Summary

7.1 This chapter is concerned with the fourth element of the new tort—the threshold of seriousness. Two distinct but related questions are considered. The first question is whether the new tort should only be actionable where the invasion of privacy was serious, and if so, how this threshold of seriousness should be set out in the new Act.

7.2 The ALRC proposes that there should be a threshold, and that it be set in the new Act using the word 'serious'.

7.3 The new Act should also provide that, in determining whether an invasion of privacy is 'serious', a court may consider whether the invasion was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff. These factors would provide a greater degree of certainty about the meaning of 'serious', while also establishing the ways in which a serious invasion of privacy may affect the plaintiff.

7.4 The second question is whether the plaintiff should be required to prove that he or she suffered 'actual damage' due to the defendant's act or conduct. The ALRC proposes that the plaintiff should not be required to prove 'actual damage'; that is, the tort should be actionable per se.

7.5 This second proposal recognises that in most cases, a serious invasion of privacy will cause emotional distress, rather than a type of harm traditionally treated by the law as 'actual damage'. Making the tort actionable per se, like an action in trespass, will enable the plaintiff to be compensated for emotional distress caused by the defendant's intentional or reckless conduct.

Seriousness

Proposal 7–1 Fourth element of action: The new Act should provide that the new cause of action is only available where the court considers that the invasion of privacy was 'serious'. The new Act should also provide that in determining whether the invasion of privacy was serious, a court may consider, among other things, whether the invasion of privacy was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff.

The need for a threshold

7.6 Some invasions of privacy should not be actionable because they are not sufficiently serious. The ALRC proposes that the new Act provide for a threshold test of seriousness that would ensure that trivial and other non-serious breaches of privacy are not actionable. The threshold the ALRC proposes is that the defendant's conduct is 'serious', having regard to whether it would be likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff.

7.7 Some threshold is arguably required by the ALRC's Terms of Reference, which ask the ALRC to design a cause of action for serious—not all—invasions of privacy.

7.8 Many privacy advocates argue that there should not be an additional threshold, and that invasions of privacy should be actionable whether or not the invasion is serious. If a person has a 'reasonable expectation of privacy' then, subject to public interest matters, some argue that the person should have an action.[1]

7.9 The NSWLRC considered that there should be no additional threshold beyond the reasonable expectation of privacy test. The nature and offensiveness of the relevant conduct were instead matters to be taken into account when determining whether an actionable invasion of privacy had occurred.[2] There is also no threshold for seriousness in the statutes of the four Canadian provinces which have a statutory cause of action for invasions of privacy.[3]

7.10 However, the ALRC considers that a threshold is a useful way to prevent people from bringing actions for non-serious invasions of privacy. The risk of non-serious actions or a proliferation of claims was raised by a number of stakeholders.[4] It is also the ALRC's view that a threshold would avoid an undue imposition on competing interests such as freedom of speech.

---

1 Eg N Witzleb, *Submission 29*; Office of the Information Commissioner, Queensland, *Submission 20*; Women's Legal Centre (ACT & Region) Inc., *Submission 19*; Pirate Party of Australia, *Submission 18*; P Wragg, *Submission 4*.

2 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) [23]–[33].

3 *Privacy Act*, RSBC 1996, c 373; *Privacy Act*, RSS 1978, c P-24; *Privacy Act*, RSNL 1990, c P-22; *Privacy Act*, CCSM 1996, c P125 (Manitoba).

4 Eg SBS, *Submission 59*; ABC, *Submission 46*; Telstra, *Submission 45*; Free TV Australia, Submission No 10 to DPM&C Issues Paper, 2011; SBS, Submission No 8 to DPM&C Issues Paper, 2011.

What should the threshold be?

7.11 If there is a threshold, where should the threshold be set, and how? One option, favoured by the ALRC, would be to set the threshold at 'serious' invasions of privacy, and invite the courts to consider a number of matters when determining whether the invasion was serious. This is a flexible option, giving the court considerable discretion. This option was favoured by the Law Institute of Victoria.

7.12 To give the courts appropriate discretion, the word 'serious' should not be defined in the new Act. However, the new Act should provide some guidance on its meaning. The word 'serious' is not a particularly precise term, and may even be interpreted to mean 'not trivial'. The ALRC considers that the threshold for this cause of action should be set higher than 'not trivial'.

7.13 Rather than define 'serious', the ALRC proposes that the new Act set out a number of factors for the court to consider when determining whether the invasion of privacy was serious. The court should consider whether the invasion was likely to be highly offensive, distressing, or harmful to a person of ordinary sensibilities in the position of the accused.

7.14 The Law Institute of Victoria suggested other factors a court may take into account when determining seriousness: the nature of the breach; the consequences of the invasion for an individual; and the extent of the invasion in terms of the numbers of individuals affected.[5] The ALRC agrees that these factors might also be relevant, but prefers the more general factors proposed above.

Objective test

7.15 The test of seriousness proposed here is an objective test. It is not about whether the plaintiff considered the invasion of privacy was serious, or about whether the effect of the invasion on the plaintiff was in fact serious.[6] Rather, it is about whether the court views the invasion as serious. One way to measure this is to ask whether the invasion of privacy was likely to have a serious effect on a person of ordinary sensibilities in the position of the plaintiff.

7.16 In this context, the ALRC suggests that 'likely' does not mean 'probable', that is, more likely than not. Rather, 'likely' means 'a real possibility, a possibility that cannot sensibly be ignored having regard to the nature and gravity of the feared harm in the particular case'.[7]

7.17 The likely effect of the conduct should also be distinguished from the actual effect of the conduct. Whether the cause of action should require proof of damage is a related question, discussed separately below.

---

5 Law Institute of Victoria, *Submission 22*.

6 Later in this chapter, the ALRC proposes that the plaintiff should not be required to prove actual damage.

7 These are the words of Lord Nicholls of Birkenhead speaking in a different context in *Re H and R (Child Sexual Abuse)* [1996] 1 FLR 80 [69] (Lord Nicholls). This definition was referred to in *Venables & Anor v News Group News Papers Ltd & Ors* [2001] EWHC QB 32 (8 January 2001) (Dame Elizabeth Butler–Sloss P). Cf *Cream Holdings Ltd v Banerjee* (2004) 1 AC 253.

Subjective element

7.18 Although usually the test of seriousness will be an objective one, in some cases, the fact that the defendant knew that the particular plaintiff was likely to be highly offended, distressed or harmed by the invasion of privacy, will also be a factor to be considered. In such circumstances, the invasion may be adjudged to be serious, even if a person of ordinary sensibilities might not have been likely to suffer such offence, distress or harm.

7.19 Section 32 of the *Civil Liability Act 2002* (NSW) provides:

> (1) A person (the defendant) does not owe a duty of care to another person (the plaintiff) to take care not to cause the plaintiff mental harm unless the defendant ought to have foreseen that a person of normal fortitude might, in the circumstances of the case, suffer a recognised psychiatric illness if reasonable care were not taken.
>
> (4) This section does not require the court to disregard what the defendant knew or ought to have known about the fortitude of the plaintiff.

7.20 The statutory cause of action for serious invasion of privacy should contain a provision similar to subsection 32(4) of the *Civil Liability Act 2002* (NSW). This provision would also be relevant to the question of the reasonable expectation of the plaintiff in their particular circumstances.

In the position of the plaintiff

7.21 It is important to ask whether the conduct was likely to highly offend, distress or harm a person *in the position of the plaintiff*. In some cases, particular attributes or circumstances of the plaintiff will mean that an invasion of their privacy will be more offensive, distressing or harmful than it might have been to another person.

7.22 In discussing whether the plaintiff had a reasonable expectation of privacy, Lord Hope, in *Campbell v MGN*, said that

> it is unrealistic to look through the eyes of a reasonable person of ordinary sensibilities at the degree of confidentiality that is to be attached to a therapy for drug addiction without relating this objective test to the particular circumstances.[8]

7.23 Lord Hope later went on to say that the Court of Appeal erred

> when they were asking themselves whether the disclosure would have offended the reasonable man of ordinary susceptibilities. The mind that they examined was the mind of the reader...This is wrong. It greatly reduces the level of protection that is afforded to the right of privacy. The mind that has to be examined is that, not of the reader in general, but of the person who is affected by the publicity. 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.[9]

---

8 *Campbell v MGN Ltd* [2004] 2 AC 457, [97] (Lord Hope).
9 Ibid [99].

7.24 Although this was said in the context of whether the plaintiff in *Campbell* had a reasonable expectation of privacy, the ALRC considers that the same reasoning should apply to the question of whether the invasion of privacy was serious. The two tests overlap, but it is clear that when applying each test, both of which are objective, it is important to consider a person in the position of the plaintiff.

Offence, distress or harm

7.25 A high likelihood or degree of offence, distress or harm is not the only indicator of the seriousness of an invasion of privacy, but it seems to be the most common.

7.26 The ALRC in 2008 and the Victorian Law Reform Commission (VLRC) in 2010 recommended that a plaintiff be required to show that the act or conduct complained of was highly offensive to a reasonable person of ordinary sensibilities.[10] The 'highly offensive' test was supported by some stakeholders.[11] A 'highly offensive' threshold is also favoured in New Zealand.[12]

7.27 Some stakeholders to this Inquiry submitted that whether the conduct was offensive is not the right test, because offence concerns emotional insult or distress, whereas the action for invasion of privacy should be concerned with affront to dignity. Offence is directed at moral outrage or wounded feeling, but seriousness should be measured by the extent of the invasion or the harm done.[13]

7.28 The ALRC is of the view that a high degree of offence is one factor to consider when assessing the seriousness of an invasion of privacy. The level of distress and harm likely to be caused by the invasion are also suitable matters to consider.[14]

7.29 Some invasions of privacy will be 'serious', despite the fact that they did not—and were not likely—to cause serious offence, distress or harm to the plaintiff. The dignitary interests of a person may be seriously infringed without the person's knowledge. For example, it may in some circumstances be a serious invasion of privacy to take or publish a photo of a person who is in a coma or a state of dementia,

---

10 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].

11 SBS, *Submission 59*; Australian Bankers' Association, *Submission 27*; Insurance Council of Australia, *Submission 15*. This threshold was supported by some stakeholders who oppose the introduction of the cause of action, perhaps because the threshold is high.

12 The New Zealand Court of Appeal has said that one of the two fundamental requirements for a successful claim for interference with privacy was publicity given to private facts 'that would be considered highly offensive to an objective reasonable person': *Hosking v Runting* (2005) 1 NZLR 1, [117]. See also *C v Holland* [2012] 3 NZLR 672 (24 August 2012) [94] (Whata J).

13 Eg N Witzleb, *Submission 29*; T Gardner, *Submission 3*.

14 Section 1 of the *Defamation Act 2003* (UK) 2013 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. It should be noted, however, that liability in defamation is strict.

despite the fact that a person in such a state is unlikely to be offended, distressed or harmed by the incident or the publication. Such invasions of privacy may be serious, even though harm to the plaintiff was unlikely or minimal.

7.30 The *Privacy Act 1988* (Cth) provides for civil penalties in cases of 'serious' or 'repeated' interferences with privacy.[15] However, the Act does not define 'serious'; the ordinary meaning of the word applies.

7.31 A seriousness threshold is also recognised in the UK. Toulson and Phipps write that unauthorised 'disclosure or use of information about a person's private life will be a violation of Art 8 only if …it is sufficiently serious to cause substantial offence to a person of ordinary sensibilities'.[16] However, this may be a low bar, intended mainly to exclude only limited or trivial disclosures. Lord Neuberger MR in *Ambrosiadou v Coward,* said that

> Just because information relates to a person's family and private life, it will not automatically be protected by the courts: for instance, the information may be of slight significance, generally expressed, or anodyne in nature. While respect for family and private life is of fundamental importance, it seems to me that the courts should, in the absence of special facts, generally expect people to adopt a reasonably robust and realistic approach to living in the 21st century.[17]

7.32 In relation to actionability for defamation, 'substantially' has been described by Tugendhat J as the lowest threshold of seriousness.[18] The ALRC proposes that the serious threshold be set higher than this.

Highly, seriously or substantially?

7.33 The ALRC proposes that an invasion of privacy should generally not be considered serious if it were only likely to cause less substantial offence, distress or harm. The relevant consideration proposed is whether the invasion of privacy was likely to be *highly* offensive, distressing or harmful.

7.34 Some stakeholders may argue that this may make the cause of action largely unattainable. Possible alternatives include that the invasion 'caused substantial offence',[19] or was 'sufficiently serious to cause substantial offence'[20] to a reasonable person of ordinary sensibilities.

---

15 *Privacy Act 1988* (Cth) s 13G.

16 RG Toulson and CM Phipps, *Confidentiality* (Sweet & Maxwell, 2012) [7–033]. Toulson and Phipps write that the other condition is that 'there is no good and sufficient reason for it—'good' meaning a reason capable of justifying the interference, and 'sufficient' meaning sufficient to outweigh the person's Art 8 rights on a balance of the legitimate competing interests'.

17 *Ambrosadou v Coward (Rev 1)* [2011] [2011] EWCA Civ 409 (12 April 2011) [30] (Lord Neuberger MR).

18 *Thornton v Telegraph Media Group Ltd* [2010] EWHC 1414 (QB).

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

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

7.35 However, the ALRC considers these alternatives might set the bar too low. Less serious invasions of privacy may be morally blameworthy, but the ALRC proposes that a higher bar be set for the purpose of imposing liability under the new tort.

Proof of damage not required

Proposal 7–2 The plaintiff should not be required to prove actual damage to have an action under the new tort.

7.36 The new tort should not require the plaintiff to prove—as an element of the tort, rather than for the purpose of awarding compensation—that he or she suffered actual damage.

7.37 The plaintiff having proved that he or she had a reasonable expectation of privacy, that the invasion of privacy was intentional or recklessly committed by the defendant and that it was serious, and the court having been satisfied that there was no countervailing interest justifying the defendant's conduct, should not then be required to prove actual damage. As discussed above, a bar must be set in part to ensure that trivial actions are not brought, but this has already been done by the earlier requirements.

7.38 In this respect, the privacy tort would be similar to other analogous intentional torts such as trespass to the person and trespass to land. In a sense, the wrong itself is the harm. The issue is then what remedy should flow from it. Some stakeholders advocated this approach to make the new privacy tort consistent with 'comparable interests such as defamation or trespass to the person'.[21] Defamation, while sometimes described as actionable per se, is however different in that damage to reputation is presumed to follow the defamatory publication.[22] There would be no presumption of damage in the new tort.

7.39 In *Tugendhat and Christie: The Law of Privacy and the Media,* the authors state that because one of the principal aims of the torts of battery, assault and false imprisonment is to 'vindicate the indignity inherent in unwanted touching, threatening, and confinement, they are actionable per se. Harm to the plaintiff is assumed.' The authors go on to state that, if

> one of the principal aims of the protection of privacy is the preservation of dignity, then consistency with trespass to the person might suggest that breaches of a reasonable expectation of privacy should also be actionable per se.[23]

---

21 N Witzleb, *Submission 29*.

22 On trespass, see RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) 40. Section 7(2) of the Defamation Act 2005 (NSW) provides that the 'publication of defamatory matter of any kind is actionable without proof of special damage': *Defamation Act 2005* (NSW) s 7(2). Note, however, that there is a defence to defamation of triviality.

23 M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [8.48].

7.40 In practice, serious invasions of privacy will usually cause emotional distress to the plaintiff. Emotional distress is not generally recognised by the common law as 'actual damage', which rather refers to personal injury, property damage, financial loss, or a recognised psychiatric illness. As a number of stakeholders submitted, the damage often caused by invasions of privacy—such as distress, humiliation and insult—may be intangible and difficult to prove.[24] PIAC submitted that a person's 'dignity is vitally important but its intrinsic nature makes it difficult to quantify in monetary terms the impact of any damage to it'.[25] Many stakeholders submitted that the action should not require proof of damage.[26]

7.41 The ALRC agrees that invasions of privacy may often cause 'only' emotional distress. If proof of actual damage as recognised by the common law were required, this would deny redress to some victims of serious invasions of privacy, and significantly undermine the value and purpose of introducing the new tort. If the goal then is to allow plaintiffs to recover damages for emotional distress, the issue is how best should the law achieve this.

7.42 One option would be to require proof of damage but define damage for the purposes of the action as including emotional distress. This would be consistent with s 52(1) of the *Privacy Act 1988* (Cth). This section 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 and humiliation suffered by the complainant.

7.43 However this approach would be inconsistent with both the well-established common law definition of actual damage and with the civil liability legislation in most states and territories (dealing with negligently inflicted mental harm).[27] The ALRC considers that the preferable approach is to make the new tort actionable per se. The threshold of seriousness will bar trivial or minor claims, and it will be rare that a plaintiff will suffer no distress from a serious invasion of privacy. In practice, if no emotional distress or actual damage has been suffered by a plaintiff, there would only be an award of damages if the circumstances of the invasion were such that there was a strong need for vindicatory damages.

---

24 N Witzleb, *Submission 29*; Law Institute of Victoria, *Submission 22*; 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.

25 Public Interest Advocacy Centre, *Submission 30*.

26 Office of the Australian Information Commissioner, *Submission 66*; NSW Young Lawyers, *Submission 58*; Women's Legal Services NSW, *Submission 57*; Queensland Council of Civil Liberties, *Submission 51*; ABC, *Submission 46*; Australian Privacy Foundation, *Submission 39*; Electronic Frontiers Australia, *Submission 44*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; B Arnold, *Submission 28*; Law Institute of Victoria, *Submission 22*; I Pieper, *Submission 6*; I Turnbull, *Submission 5*.

27 Eg *Civil Liability Act 2002* (NSW) s 31.

7.44 Some stakeholders also argued that invasions of privacy were 'abhorrent' and that it was important that the cause of action 'establish a clear deterrent'. [28] Others submitted that requiring proof of damage would burden or deter potential litigants.[29]

7.45 However, a number of stakeholders insisted that damage should need to be proved.[30] If proof of damage is not required, these stakeholders argued, there will be a proliferation of claims, many without merit, and this may lead to significant extra costs to industry.[31] For example, the Australian Subscription Television and Radio Association (ASTRA) submitted that not requiring proof of damage may 'encourage serial litigants and dubious proceedings'.[32] The Arts Law Centre of Australia also submitted that if the new tort were actionable per se, the arts and media industries would bear much of the cost of 'determining these potentially unfounded or unmeritorious claims'.[33] However, as set out above, the significant other elements of the cause of action should ensure that frivolous and unmeritorious claims are not made or successful— the action would only be available for 'serious', unjustified, invasions of privacy and only where the defendant intended to or recklessly invades the plaintiff's privacy.

7.46 The ALRC previously recommended that plaintiffs should not be required to prove damage.[34] The ALRC's proposal is also consistent with Canadian statutory causes of action.[35] It also appears that there is no requirement to prove damage in claims for disclosure of personal information under UK law, which is consistent with equitable claims for breach of an obligation of confidence. In practice this issue is not significant as most, if not all, privacy claims in the UK have been either for an injunction to prevent an invasive publication or for damages for emotional distress.

---

28 B Arnold, *Submission 28*.

29 Ibid.

30 Australian Subscription Television and Radio Association, *Submission 47*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*; Optus, *Submission 41*; Australian Bankers' Association, *Submission 27*; Office of the Information Commissioner, Queensland, *Submission 20*; Insurance Council of Australia, *Submission 15*; D Butler, *Submission 10*.

31 Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*; Insurance Council of Australia, *Submission 15*; Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011 4688; SBS, Submission No 8 to DPM&C Issues Paper, 2011; Australian Direct Marketing Association, Submission No 57 to DPM&C Issues Paper, 2011.

32 Australian Subscription Television and Radio Association, *Submission 47*.

33 Arts Law Centre of Australia, *Submission 43*.

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

35 In British Columbia, for example, '[i]t is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another': *Privacy Act*, RSBC 1996, c 373 s 1(1). See also *Privacy Act*, RSS 1978, c P-24 s 2; *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 2(2); *Privacy Act*, RSNL 1990, c P-22 s 3(1).

8. Balancing Privacy with Other Interests

Contents

Summary

8.1 This chapter considers the fifth element of the new tort. The ALRC proposes that in order for a plaintiff to have a cause of action, the court must be satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest.

8.2 This proposal recognises that privacy is not an absolute right, and that other interests may, in some cases, outweigh a plaintiff's interest in privacy.

8.3 The ALRC also proposes that the new Act should provide guidance on the meaning of 'public interest', through the inclusion of a list of public interest matters including, but not limited to, freedom of expression, freedom of the media, public health and safety, and national security.

8.4 Since the weighing of privacy interests against other interests is an element of the cause of action, a separate public interest defence is not required.

Balancing with freedom of expression and the public interest

Proposal 8–1 **Fifth element of action:** The new Act should provide that the plaintiff only has a cause of action for serious invasion of privacy where the court is satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest. A separate public interest defence would therefore not be needed.

8.5 As set out in Chapter 2, privacy is an important public interest, but of course it is not the only public interest. Sometimes, other interests should prevail over a person's interest in privacy. It is particularly important to give proper weight to competing public interests, given that Australia does not have a statutory human rights framework

or express constitutional protection of freedom of speech. Without a clear process for balancing competing interests, the new action might privilege privacy over other important interests.

8.6 Two related categories of interest are likely to compete with the plaintiff's privacy: the defendant's interest in free expression and the broader public interest.[1]

8.7 It is widely accepted that the public interest must be considered at some stage in an action for breach of privacy. What this public interest is, and how it should be considered, is discussed below. However, it is also important to note that people have a personal interest in free expression, and that this is not always less important than other people's interest in privacy. Toulson and Phipps wrote:

> Freedom of expression includes the right of people not only to express their own views but to talk about their own experiences (regardless of any general public interest), provided that it does not involve breaking a trust or confidence.[2]

8.8 The interest in free expression is a personal interest, as well as a public interest. It may have value independent of any benefit the public might have in hearing the speech. For example, a person speaking on television about their experience of being raised as an adopted child may breach the privacy of his or her parents. In such a case, it is not clear that the privacy interests of the parents necessarily outweigh the interests of the child in speaking freely about his or her life.[3]

8.9 The ALRC proposes that these competing interests be considered as part of a balancing exercise, when determining whether the plaintiff has a cause of action. The defendant's interest in freedom of expression and the broader public interest would therefore be considered at an early stage in a cause of action. Where the court considers that these interests outweigh the plaintiff's interest in privacy, the cause of action will fail.

8.10 In contrast, having a public interest as a defence would prolong the length of time an unmeritorious claim is heard. Some stakeholders noted the advantage of courts hearing the public interest issues early in proceedings. The Australian Subscription Television and Radio Association (ASTRA) submitted:

> having public interest go towards a defence is likely to prolong the length of time during which an unmeritorious claim is heard.[4]

8.11 Further, leaving public interest to be dealt with as a defence would give rise to the risk that a plaintiff could more easily use the court proceedings to stifle legitimate exposure of matters of public concern on the basis that they had a prima facie case of invasion of privacy without any consideration of the public interest at that point.

---

1 'An individual's interest in not having information about his private life published has to be set against the freedoms of others, particularly the right to freedom of expression under Art. 10, and the interests of the general public': RG Toulson and CM Phipps, *Confidentiality* (Sweet & Maxwell, 2012) [7–045].

2 Ibid [7-047].

3 Although of course it will also not necessarily be the case that the freedom of a person to tell his or her own story will necessarily outweigh the plaintiff's privacy interest. See *McKennitt v Ash* [2008] QB 73.

4 Australian Subscription Television and Radio Association, *Submission 47*.

8.12 This was the approach recommended by the ALRC in 2008 and is similar to the approach recommended by the NSWLRC in 2009.[5]

8.13 A similar balancing exercise is carried out in the UK, where rights to privacy and to freedom of expression, in Arts 8 and 10 of the European Convention on Human Rights, have been incorporated into domestic law by the *Human Rights Act 1998* (UK). Both must be considered when determining whether a cause of action for misuse of private information has been established. In making this determination, two questions are asked:

> 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?[6]

8.14 Toulson and Phipps wrote that in *Re S,* Lord Steyn 'reiterated that neither Art 8 nor Art 10 as such has priority over the other':

> When both are engaged, 'an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary'. The justifications for interfering with each right must be taken into account and an ultimate balancing exercise carried out.[7]

8.15 The balancing exercise proposed by the ALRC above is also similar to the UK approach. However, the ALRC considers that, rather than focus only on freedom of expression, a range of public interests should be considered when carrying out this balancing exercise. As proposed below, examples of these many public interests should be set out in the new Act. No one interest should have automatic priority over the privacy interest of the plaintiff.

Onus of proof

8.16 A number of stakeholders submitted that a balancing exercise should be carried out when determining actionability.[8] Others said there should instead be a public interest defence, considered later in proceedings.[9] Under the proposal above, with a balancing exercise when determining actionability, a plaintiff will have the onus of proving that their interest in privacy outweighs any competing public interests that are raised. On the other hand, if there were a public interest defence, a defendant would have the onus to prove that the defence was made out.

---

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–2; NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 26–29.

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

7 Toulson and Phipps, above n 1, [7–062], quoting *Re S (a child)* (2005) 1 AC 593, [17] (Lord Steyn).

8 Google, *Submission 54*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*.

9 In favour of a public interest defence: NSW Young Lawyers, *Submission 58*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; Australian Bankers' Association, *Submission 27*; Law Institute of Victoria, *Submission 22*; D Butler, *Submission 10*; Pirate Party of Australia, *Submission 18*; T Gardner, *Submission 3*.

8.17 The question of who should bear the onus of proof was often the main reason given by stakeholders for either supporting a public interest test in the cause of action, or a public interest defence. Many stakeholders said it was more appropriate for the defendant to bear the burden of proof, and that therefore there should be a public interest defence.[10] For example, Professor Moira Paterson submitted:

> the plaintiff already has the onus of establishing that he or she had a reasonable expectation of privacy which was breached in a serious way. The requirement that a privacy breach needs to be serious to justify litigation itself acknowledges that there is a competing interest in transparency that should always trump where the privacy breach is trivial in nature. In those circumstances it is not unreasonable to require the defendant to prove that a serious breach was nevertheless in the public interest because of the strong public interest in freedom of expression (or some other competing interest).[11]

8.18 Similarly, Peter Clarke has written that requiring consideration of the public interest when determining actionability presupposes that there must always be a public interest at stake. He writes that this is not logical and puts the cart before the horse:

> The protection of one's privacy should be separate and independent of such concerns whereas a defence may have regard to the public interest justifying such a breach. The burden should be upon the Defendant/Respondent to show there is a public interest in the intrusion. The benefit of the Victorian [Law Reform Commission's] approach is that the defence is a matter that can be considered discretely and for the defendant to crystallise what public interest is in issue.[12]

8.19 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. The VLRC argued that a plaintiff 'should not have to prove a negative, such as the lack of a countervailing public interest'.[13]

8.20 There is a public interest defence in New Zealand and Canada. New Zealand has a defence of 'legitimate public concern' to invasions of privacy.[14] The Court of Appeal of New Zealand stated, in *Hosking v Runting*:

> There should be available in cases of interference with privacy a defence enabling publication to be justified by a legitimate public concern in the information. In *P v D*, absence of legitimate public interest was treated as an element of the tort itself. But it is more conceptually sound for this to constitute a defence, particularly given the parallels with breach of confidence claims, where public interest is an established defence. Moreover, it would be for the defendant to provide the evidence of the

---

10 Eg, Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; B Arnold, *Submission 28*; Law Institute of Victoria, *Submission 22*.

11 M Paterson, *Submission 60*.

12 Peter A Clarke, Submission No 69 to DPM&C Issues Paper, 2011.

13 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 157, Recs 27, 28.

14 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].

> concern, which is the appropriate burden of proof if the plaintiff has shown that there has been an interference with his or her privacy of the kind we have described.[15]

8.21 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.[16]

8.22 In supporting a public interest defence, the law firm Maurice Blackburn has noted that a similar approach has been used for other statutory causes of action in Australia. Under the *Racial Discrimination Act 1975* (Cth), 'it is for the defendant to show that their conduct should be exempted because it has been done reasonably and in good faith for particular specified purposes'; and 'under the *Racial and Religious Tolerance Act 2001* (Vic) the defendant must demonstrate that conduct which would otherwise be racial or religious vilification was justified because it was in the public interest'.[17]

8.23 The defendant may be in a better position to provide evidence that the invasion of privacy was in the public interest. A newspaper, for example, would seem better placed to bring evidence of its own interest in free expression and the public's interest in free speech, than an individual may be to provide evidence that these interests do not outweigh the plaintiff's privacy.

8.24 However, the ALRC considers that it is preferable to consider the public interest when determining actionability, and that the plaintiff should bear the legal onus of proof on matters going to actionability. This should better ensure that privacy interests are not unduly privileged over other important rights and interests. Privacy is an interest that is relative, and the context and circumstances of the conduct are critical factors: the balancing at this stage of the action reflects this. As noted above, this approach was supported by some stakeholders. For example, Telstra submitted that

> given the seriousness of the cause of action and the potentially chilling effect it may have on business and service providers, the onus of proof should be on the plaintiff to ensure that their claim is sufficiently serious to outweigh public interest concerns at the outset.[18]

8.25 Under Proposal 8-1, the plaintiff will have the onus to prove that their privacy interest outweighs any competing public interest and the interest of the defendant in free speech. This is consistent with the general principle of law that 'a plaintiff bears

---

15 *Hosking v Runting* (2005) 1 NZLR 1, [129]. See also [130]: 'Furthermore, the scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society. A defence of legitimate public concern will ensure this. The significant value to be accorded freedom of expression requires that the tort of privacy must necessarily be tightly confined. In *Douglas v Hello!* Brooke LJ formulated the matter in the following way (at para [49]): "[A]lthough the right to freedom of expression is not in every case the ace of trumps, it is a powerful card to which the courts of this country must always pay appropriate respect."'

16 Eg *Privacy Act*, RSBC 1996, c 373, s 2(3)(a).

17 Maurice Blackburn Lawyers, Submission No 45 to DPM&C Issues Paper, 2011 (citations omitted).

18 Telstra, *Submission 45*. See also, SBS, *Submission 59*; Australian Subscription Television and Radio Association, *Submission 47*.

the burden of proving the ingredients of the cause of action', while the 'defendant bears the burden of proving the requisite elements of the defence'.[19]

8.26 The ALRC agrees with the NSWLRC when it stated in its report:

> Legal principle requires that plaintiffs bear the onus of establishing their case. It is appropriate, in our view, 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. Quite simply, privacy only needs protection if it is not outweighed, in the circumstances, by such a competing interest.[20]

8.27 However, the importance of the question of who bears the onus of proof should not be overstated and 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.[21]

8.28 In practice, facts as pleaded by the plaintiff may raise no public interest issues. It is not the case that the plaintiff would have to separately and exhaustively plead and prove the non-existence of each and every possible matter of public interest that may arise in any case involving privacy.

8.29 There is also the well-known distinction between the legal onus of proof and the evidentiary or strategic onus of proof.[22] While in general a plaintiff bears the onus of proof as to the elements of the cause of action asserted, a strategic or evidentiary onus may pass to a defendant to bring forward evidence to rebut any inferences that may be drawn from the plaintiff's case. If it does not do so, the defendant runs the strategic risk that the court may choose to draw an inference argued by the plaintiff.

A discrete exercise

8.30 The ALRC has proposed a discrete public interest balancing exercise. Another option might be to have public interest matters considered when determining whether the plaintiff had a reasonable expectation of privacy.[23]

8.31 Public interest matters will no doubt be relevant to the question of whether the plaintiff had a reasonable expectation of privacy. For example, the fact that the

---

19 C Sappideen and P Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) 355.

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

21 Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' (2011) 19 *Torts Law Journal* 104, 121–122.

22 Sappideen and Vines, above n 19, 356; CR Williams, 'Burdens and Standards in Civil Litigation' (2003) 25 *Sydney Law Review* 165.

23 That the plaintiff must have a reasonable expectation of privacy is another element of the cause of action: Proposal 8-1.

information is about a politician will be relevant to whether there is public interest in the information.

8.32 However, it may sometimes be artificial to consider public interest matters in the context of an expectation of privacy. Sometimes, a person's expectation of privacy may seem perfectly reasonable, even though the strength of a competing public interest, perhaps unknown to many reasonable people, suggests that the invasion of privacy should not be actionable.

8.33 The NSWLRC 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.[24]

8.34 Given the importance of considering competing public interests, the ALRC considers that there should be a clear and discrete public interest element in the cause of action.

Meaning of public interest

Proposal 8–2 The new Act should include the following non-exhaustive list of public interest matters which a court may consider:

(a) freedom of expression, including political communication;

(b) freedom of the media to investigate, and inform and comment on matters of public concern and importance;

(c) the proper administration of government;

(d) open justice;

(e) public health and safety;

(f) national security;

(g) the prevention and detection of crime and fraud; and

(h) the economic wellbeing of the country.

Should public interest be defined?

8.35 'Public interest' should not be defined, but a list of public interest matters could be set out in the new Act. The list would not be exhaustive, but may provide the parties and the court with useful guidance, making the cause of action more certain and predictable in scope. This may in turn reduce litigation.

---

24 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) 19.

8.36 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'.[25]

8.37 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'.[26]

8.38 Including a non-exhaustive list of public interest matters seems more helpful than a definition of public interest, which might necessarily have to be overly general or overly confined and inflexible.[27]

8.39 Community expectations of privacy change over time. This is another reason to include a non-exhaustive list of public interest matters for a court to consider, rather than a definition of public interest. It will allow the meaning of public interest to develop in line with changing community attitudes and developments in technology.

8.40 There is precedent in Australian law and in regulation for providing guidance on the meaning of 'public interest', including the public interest exemptions in the *Freedom of Information Act 1982* (Cth).[28]

8.41 A number of stakeholders expressed support for including a non-exhaustive list of factors in the Act.[29]

8.42 Other stakeholders said that the Act should not provide guidance on the meaning of public interest.[30] The Law Institute of Victoria submitted:

> This is a phrase commonly used in legislation and one with which courts are familiar. 'Public interest' is a broad concept that is flexible enough to respond to the facts and circumstances of any particular case. Given that privacy is fact and context specific, it is appropriate to keep concepts such as 'public interest' broad and flexible.[31]

8.43 Alternatively, broad concepts which go to the meaning of public interest could go in the objects section or the preamble of the Act.

---

25 *Hogan v Hinch* (2011) 243 CLR 506, [31] (citation omitted).

26 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. See also B Arnold, *Submission 28*.

27 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*.

28 *Freedom of Information Act 1982* (Cth) s 11B.

29 Office of the Australian Information Commissioner, *Submission 66*; ABC, *Submission 46*; Telstra, *Submission 45*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Public Interest Advocacy Centre, *Submission 30*.

30 Law Institute of Victoria, *Submission 22*.

31 Ibid.

Which public interests should be listed?

8.44 Article 8 of the European Convention on Human Rights, which recognises the right to respect for private and family life, provides that there should no interference by a public authority with the exercise of this right:

> except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[32]

8.45 The public interests that will perhaps most commonly conflict with a plaintiff's interest in privacy are the public interest in freedom of speech and in a free media.[33]

8.46 Many who oppose a new cause of action for privacy fear that it will impede freedom of speech and the freedom of the media. In the absence of a human rights legal framework in Australia, it seems important for the statutory cause of action for serious invasion of privacy to give express recognition to the public interest in freedom of speech and freedom of the press.

8.47 When balancing an interest in privacy with a public interest in freedom of expression, the nature of the expression will be relevant. Not all speech is of equal value to the public. Political communication, for example, should be given considerable weight in the proposed balancing exercise, particularly considering that freedom of political communication is implied in the Australian Constitution.[34]

8.48 In *Campbell,* Baroness Hale LJ said that there are 'undoubtedly different types of speech, just as there are different types of private information, some of which are more deserving of protection in a democratic society than others':

> Top of the list is political speech. The free exchange of information and ideas on matters relevant to the organisation of the economic, social and political life of the country is crucial to any democracy. Without this, it can scarcely be called a democracy at all. This includes revealing information about public figures, especially those in elective office, which would otherwise be private but is relevant to their participation in public life. Intellectual and educational speech and expression are also important in a democracy, not least because they enable the development of individuals' potential to play a full part in society and in our democratic life. Artistic speech and expression is important for similar reasons, in fostering both individual originality and creativity and the free-thinking and dynamic society we so much value. No doubt there are other kinds of speech and expression for which similar claims can be made.[35]

---

32 *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) art 8(2).

33 For many purposes, these may be the same: 'the traditional view in English law has been that freedom of the press and the freedom of individual writers are substantially the same. … However, this perspective may fail to do justice to the complexity of media freedom…' Eric Barendt et al, *Media Law: Text, Cases and Materials* (Pearson, 2013) 18–19.

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

35 *Campbell v MGN Ltd* [2004] 2 AC 457, [148]. Part of this passage was quoted by SBS, who stressed the importance of respecting the public interest in the 'free exchange of information and ideas': SBS, *Submission 59*.

8.49 Other matters of public interest may also conflict with privacy interests. The ALRC has listed some of these in Proposal 8-2.

8.50 Finally, it should be noted that privacy is also a public interest, not merely a personal interest. Although it is not included in the list proposed above which deals with *countervailing* matters of public interest, the ALRC considers that the public interest in respecting privacy should be considered in the proposed balancing exercise.

9. Forums, Limitations and Other Matters

Contents

Summary

9.1 This chapter considers a number of details in the legal design of the statutory cause of action for serious invasion of privacy, including the appropriate forums to hear the cause of action, costs orders, and limitation periods.

9.2 The ALRC proposes that federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy. The ALRC also proposes that an action under the new tort should generally be brought within one year. This is consistent with the one year limitation period prescribed for actions in defamation. It will also encourage the proper and timely administration of justice.

9.3 The chapter then discusses who should have standing to sue for a serious invasion of privacy. The ALRC proposes that the plaintiff must be a natural person,

rather than a company or other organisation. The ALRC also proposes that the statutory cause of action for serious invasion of privacy should not survive in favour of a plaintiff's estate or against a defendant's estate. These proposals reflect the fact that privacy is a matter of personal sensibility.

9.4 There may often be alternatives to bringing an action under the new tort, such as making a complaint to the Office of the Australian Information Commissioner. Failing to pursue such alternative dispute resolution processes should not bar a plaintiff from bringing an action under the new tort. However, the ALRC proposes that the new Act provide that, in determining any remedy, courts may take into account whether or not a party took reasonable steps to resolve the dispute without litigation and the outcome of any alternative dispute resolution process.

Forums

Proposal 9–1 Federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy under the new Act.

Question 9–1 If state and territory tribunals should also have jurisdiction, which tribunals would be appropriate and why?

9.5 The Terms of Reference require the ALRC to make recommendations concerning jurisdiction and access to justice. The ALRC has taken into account a range of factors including: the need to minimise confusion or inconsistency in the application of legislation across Australian jurisdictions; the range of available remedies; issues of costs of proceedings; relevant constitutional issues; and existing courts and tribunals.

9.6 In considering which forums would be appropriate to hear actions under the new tort, a number of considerations are relevant. First, is the importance of access to justice for a wide range of litigants in a wide range of circumstances. Both plaintiff and defendant interests must be considered. A number of stakeholders expressed concerns that litigation through the courts may be so expensive as to discourage plaintiffs who may be unable to afford legal representation. For example, PIAC submitted that:

> Accessibility is a key factor in considering which forum is appropriate to determine matters under a statutory cause of action for serious invasion of privacy. Otherwise, there is a risk that this type of action would become the sole preserve of those wealthy enough to afford to pay for legal representation and to run the risk of incurring an adverse costs order if they are unsuccessful.[1]

9.7 Other stakeholders similarly supported low-cost forums.[2] The ALRC notes the importance of actions for serious invasion of privacy not being prohibitively costly to the wide range of individuals who might seek redress.[3]

---

1 Public Interest Advocacy Centre, *Submission 30*.

2 Women's Legal Services NSW, *Submission 57*; Arts Law Centre of Australia, *Submission 43*; Public Interest Advocacy Centre, *Submission 30*.

3 Women's Legal Services NSW, *Submission 57*; Arts Law Centre of Australia, *Submission 43*.

9.8 Secondly, decision-makers should be able to order appropriate remedies or relief to plaintiffs. As noted by a number of stakeholders,[4] one of the most effective ways to limit the harm of an invasion of privacy is to prevent the invasion before it occurs, or to limit the effects of the invasion after it has occurred. For these purposes, an injunction will often be the appropriate remedy. Injunctive relief, however, is not available from all courts.

9.9 Lower courts and tribunals are often limited in the amount of damages that they may award. This also affects whether a particular forum is appropriate to hear an action for serious invasion of privacy.

9.10 Thirdly, an action for the new tort will frequently be brought concurrently with other actions. Where an invasion of privacy occurs through the disclosure of private information there may, for example, also be an action for breach of confidence or defamation. If it involves physical intrusion, there may also be a trespass claim. For both the plaintiff and defendant, it is preferable that all the actions arising from a particular incident be dealt with in a single forum, rather than new proceedings being required for each action. Courts may be better placed to allow multiple actions to be heard concurrently. While courts have existing jurisdiction to deal with a wide range of actions, providing powers to tribunals or other bodies to hear all other complaints related to the privacy matter would require the enactment of additional laws.

9.11 In light of these considerations, and as detailed further below, the ALRC has proposed that power to hear actions for serious invasion of privacy under the new federal statute should be vested in the Federal Court, the Federal Circuit Court, and state and territory courts. These state and territory courts would include local courts and magistrates courts where the claim is within their jurisdiction and the remedy sought is within their powers.

9.12 The ALRC has also asked for feedback on which tribunals, if any, would be appropriate forums to hear privacy actions under the new Act. The powers of various tribunals to hear these actions, as well as the possible limitations of these tribunals with respect to the action under the new Act, are discussed in more detail in the following sections.

Federal courts

9.13 The power to vest judicial power in the Federal Court of Australia (FCA) and the Federal Circuit Court of Australia (FCCA) arises under s 71 of the *Australian Constitution*. The jurisdictions of the FCA and the FCCA are generally conferred by a wide range of federal Acts such as the *Bankruptcy Act 1966* (Cth), the *Migration Act 1958* (Cth), the Australian Consumer Law,[5] the *Corporations Act 2001* (Cth), the *Telecommunications Act 1997* (Cth), and the *Privacy Act 1988* (Cth) (*Privacy Act*). As proposed in Chapter 4, the new tort should be located in a federal statute, and this statute could vest power to hear actions in the FCA and the FCCA.

---

4 National Children and Youth Law Centre, *Submission 61*; Google, *Submission 54*; Australian Privacy Foundation, *Submission 39*; B Arnold, *Submission 28*.

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

9.14 Given that many serious invasions of privacy may involve parties in different states or territories, vesting the power to hear privacy actions in courts with jurisdiction across the entire country—such as the FCA and the FCCA—may reduce the costs, time and burdens for plaintiffs.

9.15 Both the FCA and the FCCA have, in addition to jurisdiction granted to them by legislation, 'associated jurisdiction'[6] and 'accrued jurisdiction'[7] for matters, not otherwise within these courts' respective jurisdictions, that are related to matters which *are* within their respective jurisdictions. Thus, for example, while no statue confers jurisdiction on these courts for breach of contract actions, either court is able to hear a claim for breach of contract that is brought alongside, for example, a claim for misleading or deceptive conduct under the Australian Consumer Law. While associated and accrued jurisdiction would potentially mean that matters not currently within the jurisdiction of the FCA or FCCA could be heard by these courts, if brought alongside a privacy action, the ALRC does not consider this to be particularly problematic. Many related matters can already be brought before these courts—actions for defamation and negligence might be brought alongside an action arising under the *Privacy Act*, for instance.[8]

9.16 However, the ALRC considers that the FCA and the FCCA should not have exclusive jurisdiction[9] to hear actions under the new Act, as in many cases it would be less costly for litigants to use state local courts or district or circuit courts to hear proceedings.

State and territory courts

9.17 State and territory courts include Supreme Courts, District or County courts, and Local or Magistrates Courts. The new Act, as a Commonwealth law, could vest federal jurisdiction in state and territory courts to hear the new cause of action.[10]

9.18 Different powers are available to the different levels of state and territory courts. The Supreme Courts of the states and territories have general, unlimited jurisdiction.[11]

9.19 District and County Courts (and the Magistrates Court of the ACT) generally have similar powers to Supreme Courts, including powers to grant injunctions and

---

6 *Federal Court of Australia Act 1976* (Cth) s 32; *Federal Circuit Court of Australia Act 1999* (Cth) s 18.

7 *Stack v Coastal Securities (No 9)* (1983) 154 CLR 261.

8 See, eg, *Dale v Veda Advantage Information Services and Solution Limited* [2009] FCA 305 (1 April 2009).

9 The power to grant exclusive jurisdiction to federal courts is provided to the Commonwealth under s 77(ii) of the *Constitution*. For an example of exclusive jurisdiction of the Federal Court, see *Competition and Consumer Act 2010* (Cth) s 86.

10 This vesting of jurisdiction is possible under ss 71 and 77(iii) of the *Constitution* and s 39 of the *Judiciary Act 1903* (Cth) (in the cases of states), and s 122 of the *Constitution* (in the case of territories). James Crawford and Brian Opeskin, *Australian Courts of Law* (Oxford University Press, 4th ed) 57. A state or territory court will only have the power to exercise federal jurisdiction in line with ss 35 and 122 of the *Australian Constitution* where that jurisdiction power derives from a Commonwealth Act, not a state or territory act.

11 See, eg, *Supreme Court Act 1970* (NSW) s 23; *Constitution Act 1975* (Vic) s 85(1).

equitable remedies.[12] However, the jurisdiction of District and County Courts is typically limited to certain values. For example, the County Court of Victoria may only hear claims up to $200,000; the District Courts of Queensland and Western Australia, may only hear claims up to $250,000; and the District Court of NSW may only hear claims up to $750,000.[13]

9.20 The powers of Local and Magistrates Courts with respect to civil actions are often restricted in certain ways. For example, the Local Court of NSW does not have jurisdiction to hear defamation proceedings;[14] and the Magistrates Court of South Australia has powers limited to certain procedural functions, adjourning proceedings, certain statutory matter, and 'minor civil actions'.[15] Local and Magistrates Courts may have equitable jurisdiction and so may be able to hear breach of confidence actions, although this jurisdiction may be limited to cases where any relief claimed is an amount of money under a certain limit.[16] Local and Magistrates Courts typically do not have the power to grant an injunction.

9.21 While the jurisdictions of the Local, Magistrates, District and County Courts of the states and territories may in some cases have restrictions that limit their effectiveness in dealing with some privacy actions, the ALRC does not consider that there is any reason to expressly exclude these courts as possible forums for privacy actions. There would also be considerable benefit in terms of providing wider access to justice in privacy claims if these courts could hear some privacy actions.

Cost management in courts

9.22 While proceedings in courts may result in substantial costs for parties, there are mechanisms available to minimise these costs. Courts are variously empowered to direct parties to mediation, conciliation and arbitration,[17] which are designed to offer cheaper and faster dispute resolution than litigation. Courts also have the power to waive fees and, in certain cases, fees are not payable.[18] While these mechanisms will not remove the costs for all litigants, they do temper the costs associated with court proceedings in some cases.

---

12 *District Court Act 1973* (NSW) ss 44, 46; *District Court of Queensland Act 1967* (Qld) ss 68, 69; *District Court Act 1991* (SA) s 8; *County Court Act 1958* (Vic) ss 37, 49; *District Court Act 1969* (WA) ss 50, 55; *Magistrates Court Act 1930* (ACT) ss 257, 258.

13 *County Court Act 1958* (Vic) s 3, 37; *District Court of Queensland Act 1967* (Qld) s 68; *District Court Act 1969* (WA) s 50; *District Court Act 1973* (NSW) s 44.

14 *Local Court Act 2007* (NSW) s 33.

15 *Magistrates Court Act 1991* (SA) ss 8, 10, 15.

16 See, eg, *Magistrates Court (Civil Proceedings) Act 2004* (WA) s 6.

17 See, eg, the following provisions for the power to order mediation: *Federal Court of Australia Act 1976* (Cth) s 53; *Civil Procedure Act 2005* (NSW) s 26; *Civil Procedure Act 2010* (Vic) s 48(2)(c); *Supreme Court (General Civil Procedure) Rules 2005* (Vic) r 50.07.

18 *Civil Procedure Regulation 2012* No 393 (NSW) reg 11.

9.23 The ALRC has asked a question in this Discussion Paper concerning possible additions to the powers of courts to grant costs orders.[19]

Tribunals

9.24 Several states and territories have created tribunals that are able to hear civil matters, and which may be suitable forums for hearing privacy actions under the new Act. These tribunals include the ACT Civil and Administrative Tribunal (ACAT); the NSW Civil and Administrative Tribunal (NCAT); the Queensland Civil and Administrative Tribunal (QCAT); the State Administrative Tribunal of Western Australia (SAT); and the Victorian Civil and Administrative Tribunal (VCAT). These tribunals have a range of powers including, in some cases, powers to grant injunctions.[20]

9.25 The usefulness of these tribunals has been noted before—for example, the Victorian Law Reform Commission recommended that jurisdiction for privacy actions should be vested exclusively in the VCAT:

> VCAT is designed to be more accessible than the courts. It seeks to be a speedy, low-cost tribunal where legal costs do not outweigh the issues at stake. The experience in other jurisdictions demonstrates that any damages awards in cases of this nature are likely to be relatively small. The sums of money involved do not justify the level of legal costs usually associated with civil litigation in the courts.[21]

9.26 However, the power of the federal Parliament to vest federal jurisdiction in state courts under s 77(iii) of the *Constitution* may not extend to vesting jurisdiction in the ACAT, NCAT, QCAT, SAT and VCAT,[22] unless these tribunals are determined to be 'courts', for constitutional purposes.

9.27 While the ALRC considers that these tribunals may offer a useful forum for hearing privacy actions, no specific proposal is made at this stage for granting jurisdiction to a tribunal. However, the ALRC is interested in submissions from stakeholders on which civil tribunals might be appropriate.

9.28 Although federal tribunals exist, these federal tribunals do not appear to be suitable for hearing privacy actions under the new Act. Federal tribunals are limited to administrative jurisdiction. They cannot, under the *Constitution*, be granted judicial powers.[23] Moreover, the majority of these tribunals have specific areas of focus, which do not include privacy—for example, the Australian Competition Tribunal; the Copyright Tribunal of Australia; and the Migration and Refugee Review Tribunals.

---

19 See Question 11–1.

20 *ACT Civil and Administrative Tribunal Act 2008* (ACT) s 22; *Victorian Civil and Administrative Tribunal Act 1998* (Vic) s 123; *State Administrative Tribunal Act 2004* (WA) s 90 (interim injunctions only).

21 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 2010) [7.226].

22 *Victorian Civil and Administrative Tribunal Act 1998* (Vic); *NSW Civil and Administrative Tribunal Act 2013* (NSW); *Queensland Civil and Administrative Tribunal Act 2009* (Qld); *South Australian Civil and Administrative Tribunal Act 2013* (SA).

23 *R v Kirby; ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254.

9.29 The Administrative Appeals Tribunal (AAT) was suggested as a possible forum for privacy actions by some stakeholders.[24] However, although the AAT has a wide range of functions and powers, including functions under the *Privacy Act*, the functions and powers are related to the review of decisions made by administrative bodies. Some invasions of privacy may give rise to both a complaint under the *Privacy Act* and an action under the statutory cause of action for serious invasion of privacy. However, a claim based on the statutory cause of action for serious invasion of privacy, by itself, would not usually arise out of a decision by an administrative body. The AAT would therefore not be an appropriate forum to determine liability, although the existence of a civil cause of action would not prevent the plaintiff otherwise challenging a decision by an administrative body.

The role of government regulatory bodies

9.30 In addition to courts and tribunals, complaints about serious invasions of privacy might be brought through administrative bodies. The Australian Information Commissioner, in particular, has power to receive complaints from individuals who consider that a government agency or private organisation has engaged in conduct amounting to an 'interference with the privacy of an individual' by breaching the APPs.[25] The Commissioner is empowered to make a determination, including a range of declarations, such as a declaration that the respondent pay the complainant an amount by way of compensation, or that the respondent take a specified action to redress any loss or damage suffered by the complainant.[26] Similar powers are granted to state and territory information privacy commissioners.[27]

9.31 While these complaints mechanisms provide a cheaper and potentially faster dispute resolution system than courts, the ALRC does not consider that these regulatory bodies are appropriate forums to hear complaints under the statutory cause of action for serious invasion of privacy. In the absence of significant reform, the remits of these administrative bodies are typically restricted to information privacy, and to particular entities such as government agencies or large businesses. Furthermore, the possible remedies available under these complaints mechanisms are generally more limited than those available through a court, and a complainant is typically required to seek a court order to enforce a determination arising from a complaint.

9.32 However, administrative dispute resolution processes continue to play a useful role in providing cheaper, faster, and otherwise less burdensome avenues for dispute resolution.

---

24 Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Public Interest Advocacy Centre, *Submission 30*.

25 *Privacy Act 1988* (Cth) s 40.

26 Ibid s 52(1A).

27 *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).

Cause of action limited to natural persons

Proposal 9–2 The new Act should provide that the new tort be limited to natural persons.

9.33 The ALRC proposes that the statutory cause of action for serious invasion of privacy be limited to natural persons.[28] This means that corporations, government agencies or other organisations[29] would not have standing to sue for invasions of privacy. This was unanimously recommended by previous Australian law reform inquiries.[30] Actions in defamation, which are analogous to privacy actions, are also generally limited to living, natural persons.[31]

9.34 An action in privacy is designed to remedy a personal, dignitary interest. It would be incongruous to assign this interest to a corporation or other body. In *Australian Broadcasting Corporation v Lenah Game Meats,* Gummow and Hayne JJ suggested in obiter that any common law tort of privacy (were one to develop in Australian law), should be confined to natural persons as corporations lack the 'sensibilities, offence and injury … which provide a staple value for any developing law of privacy'.[32]

Non-survival of the cause of action

Proposal 9–3 A cause of action for serious invasion of privacy should not survive for the benefit of the plaintiff's estate or against the defendant's estate.

9.35 The ALRC proposes that a statutory cause of action for serious invasion of privacy be limited to living persons. The ALRC, VLRC and NSWLRC also previously recommended that a cause of action be restricted to living persons.[33] This proposal means that actions cannot survive for the benefit of a deceased person's estate, whether or not proceedings had been commenced before the death of the plaintiff. Actions also cannot subsist against the estate of a deceased person, whether or not proceedings had commenced before the death of the defendant.

---

28 Barristers Animal Welfare Panel and Voiceless, *Submission 64*.

29 Including elected bodies: *Ballina Shire Council v Ringland* (1994) 33 NSWLR 680

30 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 2010) Rec 32; ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–3(a); NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWRC Draft Bill, cl 74(1).

31 *Defamation Act 2005* (SA) s 9. Some small businesses (which employ less than 10 employees) and not for profit organisations have standing under the Act to sue for defamation.

32 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [126].

33 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008); Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 2010) Rec 32; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill, cl 79.

9.36 This provision has a similar effect to the provisions of the Uniform Defamation Laws.[34]

Privacy action protects personal interests

9.37 The new tort is intended to remedy the wrong to a person's dignitary interests. It should therefore be limited to living persons.[35] This position is in keeping with the common law rule of *actio personalis moritur cum persona* (a personal action dies with the plaintiff or the defendant).[36]

9.38 Given the personal nature of a privacy action, the ALRC considers that only the individual who has suffered loss or damage should be able to sue for relief. An action cannot therefore be commenced, or continued, by the legal personal representative of the deceased person.

9.39 The so-called 'mischief' to be remedied by a privacy action is the mental harm and hurt to feelings suffered by a living person.[37] PIAC noted that:

> Most existing statutory causes of action for invasion of privacy lapse with the death of the person whose privacy has allegedly been invaded. This can be seen as flowing from the fact that the right to privacy is generally seen as a personal right. It has also been justified on the basis that because the main mischief of an invasion of privacy is the mental harm and injured feelings suffered by an individual, only living individuals should be allowed to seek relief.[38]

9.40 A statutory cause of action for serious invasion of privacy is analogous to an action in defamation, which does not survive the death of the person defamed, nor the person who published the defamatory matter.[39] The Law Institute of Victoria made the distinction between actions in defamation and actions for breach of confidence, arguing that a duty of confidence can persist after death.[40] However, breach of confidence actions protect quasi-proprietorial interests, that is, the plaintiff's interest in the confidential information, which will often be commercial information. By contrast, privacy actions protect a personal interest in the plaintiff's privacy.

9.41 Several stakeholders, however, support the principle of the survival of the action.[41] However, even where actions survive for the benefit of an estate, the relevant legislation generally restricts the damages recoverable to special damages for the precisely calculated pecuniary losses suffered as a result of actual damage from injuries received, such as medical expenses or loss of earnings before death and does not allow damages for pain and suffering and the like.[42]

---

34 Eg, *Defamation Act 2005* (NSW) s 10.The Tasmanian Act does not include this provision.
35 Several stakeholder supported this position: Insurance Council of Australia, *Submission 15*; Arts Law Centre of Australia, *Submission 43*; Telstra, *Submission 45*.
36 RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [11.53], [28.38].
37 Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy*, (2004) [29].
38 Public Interest Advocacy Centre, *Submission 30*.
39 See, eg, *Defamation Act 2005* (SA) s 10.
40 Law Institute of Victoria, *Submission 22*.
41 Australian Privacy Foundation, *Submission 39*.
42 *Law Reform (Miscellaneous Provisions) Act 1946* (NSW) s 2.

9.42 Some stakeholders submitted that the action could survive in some specific circumstances.[43] For example, PIAC argued that the action should survive the death of a plaintiff where 'important systemic issues are involved'.[44] By way of example, PIAC pointed to anti-discrimination complaints which, in NSW, survive the death of a complainant.[45] PIAC suggested that the value of privacy as a matter of public interest is akin to the public value in eliminating discrimination and should thus survive the death of a complainant for the good of all society. It could be argued, however, that any damages payable to an estate for an invasion of the privacy of a now deceased individual are a windfall to the estate and the beneficiaries who may not have been harmed in any way by an invasion of privacy.

Impact on family member's privacy

9.43 Given that a privacy action generates a personal right of action, it follows that an action should not be designed to remedy any secondary damage others might suffer—for example, a surviving family member who has suffered distress caused by the invasion of the deceased person's privacy while he or she was alive. However, there may be instances where the conduct of a defendant following the death of an individual may invade the privacy of surviving relatives or other parties who are closely involved. It is important to note that the non-survival of a deceased person's action does not mean that family members or other parties are unable to pursue their own actions for serious invasion of privacy where they meet the tests for actionability in their own right.[46] These actions may arise out of conduct indirectly involving a deceased person, such as where the privacy of a family member or other relevant party is invaded in a private moment of grief or mourning,[47] or in circumstances where a deceased's medical record is published to disclose a condition affecting surviving relatives.

9.44 Another example, outlined in PIAC's submission, is where a so-called tribute or dedication page to a deceased person established on a social media site such as Facebook reveals personal information about a third party.[48] These circumstances may generate a cause of action for the third party. This position is generally in line with defamation law where a family member may only bring an action in respect of a defamatory slur against a deceased family member where he or she has been personally defamed.[49]

Representative actions by affected parties

9.45 The Arts Law Centre of Australia and the Law Institute of Victoria argued that an action should survive the death of the person whose privacy is invaded if that person identified as being Aboriginal or Torres Strait Islander, given the specific cultural

---

43 I Turnbull, *Submission 5*.
44 Public Interest Advocacy Centre, *Submission 30*.
45 *Anti-Discrimination Act* (NT) s 93(1).
46 SBS, *Submission 59*; NSW Young Lawyers, *Submission 58*; Australian Subscription Television and Radio Association, *Submission 47*.
47 NSW Young Lawyers, *Submission 58*; Public Interest Advocacy Centre, *Submission 30*.
48 Public Interest Advocacy Centre, *Submission 30*.
49 *Krahe v TCN Channel Nine Pty Ltd* (1986) 4 NSWLR 536.

beliefs of those communities associated with mourning and death.[50] In these cases, a family or other affected party would bring the claim on behalf of the deceased person. However, the ALRC considers that the wrong for which action may be brought is committed against the individuals whose privacy has been invaded.

9.46 There is some guidance at law about representative actions brought by affected parties. The *Australian Securities and Investments Commission Act* 2001 (Cth), for example, provides for a court to make orders that apply to a class of 'affected individuals', even where those individuals are not subject to the proceedings.[51] In consumer class actions or data breaches where plaintiffs can be easily identified, such a provision may well be useful. However, in the highly personal context of invasions of privacy, identifying relevant or affected parties to a representative action may be difficult.

9.47 The Law Institute of Victoria submitted that remedies could be limited to 'those that protect the deceased's identity, for example, to allow corrective orders and declarations but not damages'.[52] The Australian Privacy Foundation argued that a court may consider the financial circumstances of a deceased defendant when awarding remedies against their estate.[53] However these considerations would require valuation of a deceased's estate, and may lead to lengthy and costly legal disputes over the administration and distribution of a defendant's estate, tying up the estate and leaving creditors and beneficiaries waiting many years for distribution.

9.48 The Law Society of NSW Young Lawyers' Committee on Communication, Entertainment and Technology recommended vesting power to bring actions on behalf of a deceased person in the OAIC.[54] This approach would require significant reform of the operation of the *Privacy Act* including, but not limited to, broadening the powers of the OAIC to consider privacy matters beyond information privacy and removing the various exemptions to the Act. It may also conflict with the independent and impartial role of the OAIC as conciliators of privacy complaints.

International consistency

9.49 Limiting the action for statutory invasion of privacy to living persons would, generally speaking, bring Australian law into line with international privacy law.[55] PIAC noted, however, the exception of French law which allows family members to bring civil privacy actions on behalf of a deceased relative.[56] An example is the 2007 case of *Hachette Filipacchi Associés (Paris-Match) v France.*[57]

---

50 Arts Law Centre of Australia, *Submission 43*; Law Institute of Victoria, *Submission 22*.

51 *Australian Securities and Investments Commission Act 2001* (Cth) s 12GNB. The OAIC highlighted this provision in its submission as a possible model for matters which impacted on the privacy of a large group of individuals.

52 Law Institute of Victoria, *Submission 22*.

53 Australian Privacy Foundation, *Submission 39*.

54 NSW Young Lawyers, *Submission 58*.

55 See, eg *Privacy Act*, RSBC 1996, c 373 s 5.

56 Public Interest Advocacy Centre, *Submission 30*.

57 *Hachette Filipacchi Associés (Paris-Match) v France* (2009) 49 EHRR 515.

Representative and class actions

9.50 Several stakeholders raised the issue of representative or class actions, arguing that the availability of these mechanisms in the new statutory tort would strengthen access to justice.[58] The ALRC supports the principle of access to justice, noting it is a Term of Reference for this Inquiry. However, the ALRC has not made a proposal on representative or class actions as existing mechanisms would apply to the statutory tort in the same way they apply to other civil actions. For instance, Part IVA of the *Federal Court Act* 1976 (Cth) provides a framework for representative proceedings to the Federal Court.

9.51 The Office of the Public Advocate (Queensland) submitted that the ALRC should consider ways to accommodate a litigation guardian to conduct legal proceedings on behalf of an adult with impaired decision-making capacity.[59] The ALRC also considers that this is an important issue concerning access to justice, but that it requires broader consideration than its application just to the proposed new statutory tort. The ALRC is currently undertaking an inquiry into equality, capacity and disability in Commonwealth laws. That inquiry is considering, among other things, the role of litigation guardians in civil proceedings. Its proposals would have relevance and application to any new statutory cause of action.[60]

Limitation period

Proposal 9–4 A person should not be able to bring an action under the new tort after either (a) one year from the date on which the plaintiff became aware of the invasion of privacy, or (b) three years from the date on which the invasion of privacy occurred, whichever comes earlier. In exceptional circumstances the court may extend the limitation period for an appropriate period, expiring no later than three years from the date when the invasion occurred.

9.52 The ALRC proposes a primary limitation period of one year from the date a plaintiff became aware of the invasion, with the discretion for a court to extend this period to up to three years from the date the invasion occurred.[61]

9.53 Previous law reform inquiries have diverged on this issue. The NSWLRC proposed a one year limitation period, in line with actions in defamation.[62] In contrast,

---

58 Office of the Australian Information Commissioner, *Submission 66*; B Arnold, *Submission 28*; Pirate Party of Australia, *Submission 18*.

59 Office of the Public Advocate (Queensland), *Submission 12*.

60 *Equality, Capacity and Disability in Commonwealth Laws* <www.alrc.gov.au/inquiries/legal-barriers-people-disability>.

61 Several stakeholders supported this proposal: SBS, *Submission 59*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*; Arts Law Centre of Australia, *Submission 43*; Optus, *Submission 41*; T Gardner, *Submission 3*.

62 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Para. 9.1.

the VLRC proposed a three year limitation period, consistent with actions for personal injury.[63]

Ensure fairness and certainty to both parties to a proceeding

9.54 A one year limitation period will assist in providing fairness to both parties to a proceeding and encourage the proper and timely administration of justice. A relatively short limitation period will balance the interests of both parties to a proceeding, providing adequate time for a plaintiff to appreciate and manage the emotional and financial repercussions of a serious invasion of privacy, while also providing certainty and a timely opportunity to defend proceedings to defendants.

9.55 It would be burdensome on defendants if the existence of a longer limitation period led to uncertainty and anxiety as to whether they are likely to be sued. Preparing a defence case and calculating the likely cost of litigation and possible remedies may be more challenging the longer a plaintiff takes to initiate proceedings.

9.56 Some stakeholders have raised the concern that extending a limitation period beyond one year may encourage plaintiffs to delay bringing an action.[64] The Australian Subscription Television and Radio Association (ASTRA) argued that a plaintiff may be motivated to delay an action in order to exacerbate the damage caused by the invasion with a view to increasing a possible award of damages.[65] There is a legitimate policy rationale in designing law in a way that encourages plaintiffs to act reasonably quickly to initiate proceedings. This approach is also in the interests of plaintiffs who should seek to reduce the possibility of escalating or exacerbating an invasion of privacy by bringing an action as quickly as possible.

9.57 The ALRC considers a primary one year limitation period best balances the interests of plaintiffs (in being afforded sufficient time after discovering a breach to investigate and organise their claim) with the interests of defendants (in being able to arrange their affairs knowing that claims will not be brought against them after a particular period of time).

Consistency with comparable causes of action

9.58 This proposal is consistent with the one-year limitation period prescribed for actions in defamation.[66] Consistency with the position in defamation law may avoid the risk that plaintiffs will forum-shop between comparable actions. A one year limitation period is also consistent with the limitation period for defamation actions in the UK.[67]

9.59 The rationale for one year limitation periods in defamation is applicable to privacy actions. Defamation actions are based on damage to a person's reputation, a

---

63 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 2010) Para. 7.248; ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008).

64 Australian Subscription Television and Radio Association, *Submission 47*; Arts Law Centre of Australia, *Submission 43*.

65 Australian Subscription Television and Radio Association, *Submission 47*.

66 See, eg, *Limitation Act 1969* (NSW) s 14B.

67 *Limitation Act 1980* (UK) s 4A.

harm which is complete on publication. Arguably, the act of publication should be apparent to a litigant in defamation actions as the media has a significant and visible presence in contemporary life. The same logic can be applied to privacy actions, as a serious invasion of privacy is likely to be more apparent than in other civil causes of action. This is particularly compelling given the high threshold for actionability where a plaintiff must demonstrate a *serious* invasion of privacy. It is probable that a serious invasion of privacy will be immediately evident to a plaintiff. A short limitation period would not therefore hinder a plaintiff's capacity to commence proceedings.

9.60 In contrast to actions in defamation, actions in personal injury, which generally have a longer limitation period of three years, are based on injury to the individual which may take longer to eventuate.

9.61 This proposal is also consistent with the limitation periods in the *Privacy Act* with respect to when the OAIC can hear complaints.[68] A complaint of privacy interference by an APP entity can be made within 12 months from the date the applicant becomes aware of the relevant act or conduct.[69] The OAIC then has discretion as to whether or not to investigate a complaint of privacy interference made after this date. The OAIC supports the application of a similar limitation period to a statutory cause of action for serious invasion of privacy.[70]

9.62 Several stakeholders suggested that a longer time period, closer to the three year limitation period for personal injury actions,[71] would be more appropriate.[72] These stakeholders suggested that an individual whose privacy has been seriously invaded may be too distressed to consider legal avenues for redress within a one year period. The ALRC considers this to be an important consideration to be taken into account by a court when considering whether an extension on the limitation period is reasonable in all the circumstances.

Commencement of limitation period

9.63 The ALRC considers the limitation period should start when the complainant becomes aware of the invasion of privacy.[73] The OAIC submitted that applicants may be unaware they have experienced a serious invasion of privacy for some period after the event, due to advances in communication and surveillance technology.[74] These developments in technology mean that plaintiffs may not be immediately aware of the disclosure of their private information on the internet, or the use of covert and unlawful surveillance devices to monitor their private activities.

---

68 *Privacy Act 1988* (Cth) s 41(1)(c).
69 Office of the Australian Information Commissioner, *Submission 66*.
70 Ibid.
71 See, eg, *Limitation Act 1969* (NSW) s 18A.
72 Law Institute of Victoria, *Submission 22*; Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy*, (2004) Rec 28.
73 N Witzleb, *Submission 29*.
74 Office of the Australian Information Commissioner, *Submission 66*.

9.64 SBS argued that the limitation period should commence from the date of disclosure or publication of the private information.[75] As previously outlined, this is in keeping with defamation law. Publication of an individual's private information in the mainstream media will, necessarily, be relatively obvious to a plaintiff. However, the ALRC considers it would be unfair to restrict individuals from pursuing a civil claim in privacy in circumstances where the invasion is less obvious, but still serious.

9.65 It is important to consider the interaction of the limitation period with other elements of the cause of action. The ALRC proposed that the tort for serious invasion of privacy should be actionable per se. Commencing the limitation period from the date when the plaintiff became aware of the invasion will not conflict with this element of the cause of action as a plaintiff will not have to demonstrate harm or damage suffered at a particular time.

Extension of limitation period

9.66 The ALRC's proposal provides a court with the discretion to extend a limitation period where there are reasonable circumstances for a plaintiff's delay in initiating proceedings. This proposal provides a degree of flexibility to courts and parties to a proceeding, ensuring protection for plaintiffs and allowing for the fair and timely resolution of meritorious claims.

9.67 This proposal is in keeping with the recommendations of the NSWLRC.[76] It is also consistent with defamation law which provides that a court may allow an extension of up to three years from the date of publication of the defamatory matter, 'if satisfied that it was not reasonable in the circumstances for the plaintiff to have commenced an action in relation to the matter complained of within 1 year from the date of the publication'.[77]

9.68 This position is also consistent with the UK's approach to defamation actions. Under the *Limitation Act* 1980 (UK),[78] a UK court may extend limitation periods where it would be 'prejudicial' to a plaintiff and/or to a defendant to restrict the period to one year. In making an order for an extension of time, a court must have regard to all the circumstances of the case and in particular to the length of the delay and the reasons for the delay.[79] The ALRC considers this a useful model for Australian courts.

9.69 There is precedent at common law and statute in Australian jurisdictions for courts to grant extensions on limitation periods. The factors a court may consider in granting an extension include: whether the justice of the case requires that the application be granted; whether a fair trial is possible by reason of the time that has elapsed since the events giving rise to the cause of action; the length of delay and any

75 SBS, *Submission 59*.
76 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [9.1].
77 *Limitation Act 1969* (NSW) s 56A; *Defamation Act 2005* (SA) s 56A.
78 *Limitation Act 1980* (UK) s 32A.
79 Ibid s 32A(2).

explanation for it are relevant considerations; and whether a respondent is prima facie prejudiced by being deprived of the protection of the limitation period.[80]

Alternative dispute resolution processes

Proposal 9–5 The new Act should provide that, in determining any remedy, the court may take into account:

(a) whether or not a party took reasonable steps to resolve the dispute without litigation; and

(b) the outcome of any alternative dispute resolution process.

9.70 Complaints about serious invasions of privacy may be made to statutory bodies. These include, in particular, to the Office of the Australian Information Commissioner (the OAIC), the Australian Communications and Media Authority (the ACMA), state and territory privacy commissioners and ombudsmen. Various industry bodies also provide alternative dispute resolution processes.

9.71 These alternative dispute resolution (ADR) processes offer several advantages over judicial proceedings. In particular, they may be cheaper and faster than judicial proceedings, and they may be less emotionally burdensome on the parties involved. The use of ADR may also reduce the case load of courts, which is desirable for the efficient administration of justice.

9.72 If a statutory cause of action for serious invasion of privacy is enacted, the availability of these existing dispute resolution processes should be recognised. Some possibilities include requiring a complainant to pursue some other form of dispute resolution before commencing judicial proceedings, prohibiting judicial proceedings if ADR has been undertaken, or prohibiting ADR if judicial proceedings have been undertaken.

9.73 For reasons set out below, the ALRC has concluded that a complainant should not be required to pursue ADR before initiating judicial proceedings. Nor should they be barred from initiating judicial proceedings where ADR has previously been pursued. The ADR and judicial processes should remain independent, although the fact that an individual has pursued one process might be taken into account in another process.

No requirement to pursue ADR

9.74 That the use of some form of ADR should be encouraged is widely acknowledged. However, stakeholders took different views on whether or not ADR prior to judicial proceedings should be mandatory. Several stakeholders supported mandatory ADR,[81] and a number supported only voluntary ADR.[82]

---

80 *Brisbane South Regional Health Authority v Taylor* (1996) 186 CLR 541.

81 Optus, *Submission 41*; Australian Bankers' Association, *Submission 27* 47; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*.

9.75 There would be several difficulties in requiring plaintiffs to pursue ADR before initiating judicial proceedings. Although there is a range of ADR options available, the various options are often limited to specific types of matters. For instance, the OAIC may investigate complaints relating to data protection under the *Privacy Act*; state and territory commissioners and ombudsmen may investigate complaints relating to state and territory agencies; and the ACMA may investigate complaints relating to media and communications organisations. There is at present no single ADR forum that is empowered to deal with all types of complaints that might lead to proceedings under a statutory cause of action for serious invasion of privacy. A requirement that potential plaintiffs pursue ADR before initiating judicial proceedings may therefore be too onerous, requiring them to research a complex and fragmented landscape to determine which ADR option would apply in their case.

9.76 Moreover, barring potential plaintiffs from initiating ADR without first pursuing non-judicial proceedings would present a significant restriction on the potential plaintiffs' access to justice. This would be particularly problematic where the individual wished to seek an injunction, or where the defendant would be unlikely to engage in ADR in good faith—in either case, the plaintiff would be faced with additional time and financial costs with little chance of obtaining appropriate redress.

9.77 Mandatory ADR may also be inappropriate in cases where one party poses a serious threat, including a serious psychological or emotional threat, to the other party. Several stakeholders argued that this would be a particular problem in many privacy cases involving domestic violence.[83]

9.78 Rather than a general requirement that potential plaintiffs pursue ADR processes before initiating judicial proceedings, it is preferable to use existing court powers to refer matters to dispute resolution where appropriate (and other existing provisions relating to dispute resolution in court rules).[84] This would allow the courts to take into account the urgency of a matter, the relationship between the parties, and any other factors relevant to whether such an order should be made. However, possible administrative dispute resolution providers, such as the OAIC and the ACMA, may require specific powers in order to receive court-referred disputes. As the OAIC noted, under the current *Privacy Act*,

> It would not be appropriate for the OAIC to take on an alternative dispute resolution role in the absence of a complaints model being adopted. For example, the OAIC suggests it would not be workable for a court to refer matters to the OAIC for conciliation. In particular, this is because the OAIC relies to some extent on the investigative powers in Part V of the *Privacy Act* in order to successfully conduct its

82 SBS, *Submission 59*; Women's Legal Services NSW, *Submission 57*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; B Arnold, *Submission 28*; C Jansz-Richardson, *Submission 24*; T Gardner, *Submission 3*.

83 Women's Legal Services NSW, *Submission 57*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; Women's Legal Centre (ACT & Region) Inc., *Submission 19*.

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

> conciliations, and those investigative powers would not be triggered in such circumstances.[85]

No bar on judicial proceedings after ADR

9.79 The ALRC has not proposed that a complainant who has received a determination from an ADR process should be barred from initiating judicial proceedings about the same matter.

9.80 While it may be undesirable to have individuals 'double-dipping' by receiving successful outcomes from a non-judicial process as well as judicial proceedings, a statutory bar on judicial proceedings after a non-judicial process would present a serious limitation on access to justice and discourage the use of non-judicial processes.

9.81 The risks of a complainant double-dipping would likely be minimal. An unsuccessful ADR process would generally be a strong indicator that an action under the statutory cause of action would be unsuccessful as well.

Courts empowered to take account of non-judicial proceedings

9.82 In order to encourage the use of ADR and to ensure that inappropriate double-dipping is kept to a minimum, courts should be empowered, when determining any remedies under the statutory cause of action for serious invasion of privacy, to take into account: (i) whether or not parties to proceedings have undertaken ADR in good faith; and (ii) the outcome of that non-judicial process, including the award of any monetary remedy.

---

85 Office of the Australian Information Commissioner, *Submission 66*.

10. Defences and Exemptions

Contents

Summary

10.1 The plaintiff's right to succeed under the new tort will be limited by appropriate defences. Defences reflect the need to protect important countervailing interests, whether they are interests of a personal or public nature. Defendants will bear the onus of proving that their conduct is subject to a defence or exemption.

10.2 This chapter begins with a defence of lawful authority. This defence will arise where, for example, law enforcement agencies rely on their statutory authority to carry out an act which would invade a person's privacy.

10.3 The ALRC also proposes a defence for conduct that was incidental to the exercise of a lawful right of defence of persons or property where the conduct was proportionate, necessary and reasonable.

10.4 This chapter considers the desirability of a defence of necessity. The ALRC has not made a proposal for this defence, instead posing a question to stakeholders.

10.5 The ALRC proposes a number of defences which are the same as, or analogous to, defamation defences: absolute privilege; qualified privilege; publication of public

documents; and fair and accurate reporting of public proceedings. These defences reflect the need to protect defendants in privacy actions from liability which would stifle legitimate reporting, debate and discussion.

10.6 There are some factors which the ALRC considers would be more appropriately considered when the court is determining whether a plaintiff has a reasonable expectation of privacy. The ALRC has not therefore proposed the following as defences: material in the public domain; consent; or public interest. As in the case of other intentional torts, contributory negligence will not be a defence.

10.7 This chapter includes a proposal for a safe harbour exemption for internet intermediaries which would exempt internet hosts and platform providers from liability provided they meet certain conditions. The ALRC is interested in stakeholder feedback on the form and content of a safe harbour exemption.

Lawful authority

Proposal 10–1 The new Act should provide a defence of lawful authority.

10.8 The defence of lawful authority provides government agencies, security and intelligence organisations, and law enforcement agencies with protection from liability for serious invasions of privacy where that conduct was consistent with their statutory powers.[1]

10.9 This defence is consistent with the principle that any licence for public bodies or officials to pursue conduct which may infringe the rights or interests of an individual must be clearly and unambiguously justified in legislation. In *Coco v R* a majority of the High Court of Australia explained this so-called principle of legality:

> Statutory authority to engage in what otherwise would be tortious conduct must be clearly expressed in unmistakeable and unambiguous language...The insistence on express authorisation of an abrogation or curtailment of a fundamental right, freedom or immunity must be understood as a requirement of some manifestation or indication that the legislature has not only directed its attention to the question of the abrogation or curtailment of such basic rights, freedoms and immunities, but also determined upon abrogation or curtailment of them.[2]

10.10 The analogous defence of statutory authority to intentional torts protects individuals and agencies from civil suits where a defendant's conduct was committed in order to prevent and detect crime; in exercise of powers of arrest; and in the provision of public utilities and services.[3]

---

1 A number of stakeholders supported this defence: SBS, *Submission 59*; NSW Young Lawyers, *Submission 58*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; ABC, *Submission 46*; Australian Bureau of Statistics, *Submission 32*; Public Interest Advocacy Centre, *Submission 30*; B Arnold, *Submission 28*.

2 *Coco v The Queen* [1994] HCA 15 (13 April 1994) [8]–[9] (Mason CJ, Brennan, Toohey, Gaudron and McHugh JJ).

3 RP Balkin and JLR Davis, *Law of Torts* (Butterworth Law, 5th ed, 2009) [6.49].

10.11 The NSWLRC noted that this defence is necessary to enable state agencies, such as the Australian Federal Police (AFP), to carry out their functions in a manner consistent with the protection of public interests such as security and public order.[4] The ALRC recognises that activities that may otherwise amount to an invasion of privacy may be justified where the invasion was necessary for law enforcement purposes.[5]

10.12 The AFP provided examples of legal requirements which may involve the authorised procurement of an individual's private information.[6] For example, the *Australian Federal Police Act 1979* (Cth)[7] requires the AFP to safeguard the interests of the Commonwealth, prevent crime and protect persons from injury, death and property damage. The AFP stated that

> undertaking these activities will inevitably involve interfering with an individual's privacy on occasions. Where this does occur every effort is made to respect an individual's privacy by ensuring the information that is obtained is properly protected and dealt with whilst in the possession of the AFP. Indeed, the various Acts contain provisions which set out how the information can be used by law enforcement agencies and how it must be protected.[8]

10.13 The AFP submitted that their activities are already subject to a range of existing internal and independent 'accountability frameworks'.[9]

10.14 However, the ALRC considers the statutory cause of action would provide personal redress for individuals whose privacy has been invaded, where an agency acts outside their lawful authority.

10.15 The AFP raised the concern that the risk of liability may lead to unmeritorious litigation which could divert resources away from important law enforcement and security operations.[10] However, the ALRC considers that the thresholds built into the design of the statutory cause of action, including the requirement that the conduct was serious, will prevent unmeritorious claims proceeding to trial.

10.16 The AFP also raised the concern that not exempting law enforcement from liability may inhibit the legitimate and lawful activities of law enforcement and intelligences agencies, causing agencies to change established and efficient modes of operation.[11] Similarly, the process of having to adduce evidence of intelligence gathering methods may disclose the lawful, covert practices of law enforcement and intelligence organisations and may reveal the identity of individuals under surveillance

---

4 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 43.

5 Eg, closed-circuit television (CCTV) and mobile phone records may be valuable sources of evidence in criminal investigations: *The Queen v Bayley* [2013] VSC 313 (19 June 2013).

6 Australian Federal Police, *Submission 67*.

7 Australian Federal Police Act 1979 (Cth).

8 Australian Federal Police, *Submission 67*.

9 Ibid. These frameworks include s 180F of the *Telecommunications (Interception and Access) Act* 1979 (Cth) (TIA Act) which requires the AFP to consider whether any interference with privacy may result through the disclosure of information. Similarly, s 46(2)(a) of the TIA Act requires a judge or AAT member to consider whether an individual's privacy would be interfered with by interception through the use of a warrant.

10 Australian Federal Police, *Submission 67*.

11 Ibid.

or investigation. The ALRC considers however, there are strong protections at current law to mitigate this risk. These protections include closed court proceedings and other measures provided by federal, state and territory court acts.[12]

Meaning of 'lawful authority'

10.17 The ALRC has not provided guidance on the meaning of 'lawful authority', as this may well be a drafting issue. However, the ALRC welcomes stakeholder responses on the wording of this defence, with consideration to whether the exception should be clarified.

10.18 When considering the meaning of the phrase 'required or authorised by or under law' in its previous privacy Inquiry, the ALRC recommended that the defence include authority under Commonwealth, state and territory acts and delegated legislation; a duty of confidentiality under common law or equity; an order of a court or tribunal; and documents that are given the force of law by an Act, such as industrial awards'.[13]

10.19 In this Inquiry, the ALRC considers that 'lawful' should give effect to the above legislative and non-legislative instruments. 'Lawful' should also extend to documents which have the 'force of the law'. The ALRC's previous Inquiry found that a document may have the 'force of law' if it is an offence to breach its provisions, or it is possible for a penalty lawfully to be imposed if its provisions are breached.[14] This would include warrants obtained by law enforcement pursuant to a relevant act.

10.20 The term 'authority' implies discretion to pursue certain lawful conduct, and may apply to a wide range of acts or practices.[15]

10.21 Dr Normann Witzleb argued that the defence of lawful authority is unnecessary as where an authorised person exercises their statutory authority, they are necessarily authorised to commit that action.[16] However the ALRC considers clear legislative direction as to the interaction of a statutory cause of action for serious invasion of privacy with the activities of law enforcement agencies will provide certainty to parties.

10.22 The availability of a defence of lawful authority is consistent with previous law reform inquiries.[17]

10.23 In light of new technologies and recent revelations of surveillance and data sharing by public agencies, there is a strong community expectation that public agencies should not be exempt or immune from liability for serious invasions of privacy.

---

12 Eg, *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).
13 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [13.44].
14 Ibid [16.22].
15 Ibid [16.72].
16 Witzleb, *Submission 29*.
17 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.194]; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009); ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008).

Incidental to lawful rights of defence

Proposal 10–2 The new Act should provide a defence for conduct incidental to the exercise of a lawful right of defence of persons or property where that conduct was proportionate, necessary and reasonable.

10.24 This defence protects individuals from liability where a serious invasion of privacy was necessary to prevent a threatened or actual harm, and where their response to that harm was reasonable.[18] This defence will arise where the defendant has reasonable grounds for apprehending a threat of harm to persons or property. The defence will arise in several circumstances: self-defence; defence of another person; and defence of property. The requirement that the conduct be proportionate, necessary and reasonable is an important qualification. At tort law, the question of whether a defendant's conduct was reasonable is a question of fact.[19]

10.25 This defence will protect an individual from liability where they act in self-defence. Civil liability legislation around the country provides an analogous protection for self-defence where the conduct to which the person is responding was unlawful and where:

> (2) A person carries out conduct in self-defence if and only if the person considers the conduct is necessary:
>
> (a) to defend himself or herself or another person, or
> (b) to prevent or terminate the unlawful deprivation of his or her liberty or the liberty of another person, or
> (c) to protect property from unlawful taking, destruction, damage or interference, or
> (d) to prevent criminal trespass to any land or premises or to remove a person committing any such criminal trespass,
>
> and the conduct is a reasonable response in the circumstances as he or she perceives them.[20]

10.26 The defence will also protect individuals from liability where their conduct protects a third party from harm particularly where that third party is under the individual's care or responsibility, or where that third party is incapable of exercising self-defence. This may involve the protection of children and young people, vulnerable groups or animals. The defence of the person of another operates at tort law and has been codified in some Australian jurisdictions.[21] At common law, the defence extends

---

18 Similar defences were recommended by the VLRC, ALRC and NSWLRC: Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 27b; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.2]; ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–4.

19 Balkin and Davis, above n 3, [6.15].

20 Eg *Civil Liability Act 2002* (NSW) s 52.

21 *Criminal Code* (Cth) cl 10.4.

to protection of an individual's household, employer, family members and even, in some circumstances, strangers.[22]

10.27 The defence would also protect individuals from liability where their conduct was incidental to the defence of property in situations where another person threatens to commit, or does commit, trespass to property. This is analogous to the defence for intentional torts where a defendant's conduct in response to the threat or harm to their property is reasonable.[23]

10.28 The defence that conduct was incidental to the defence of persons or property operates in Canadian law. It has been used in Canada to protect defendants from liability in the following situations: where an employer used covert surveillance to monitor an employee whom the employer reasonably suspected of stealing stock; and where an individual intercepted a neighbour's phone to gain evidence of blackmail.[24]

10.29 The Insurance Council of Australia proposed a defence that 'the act or conduct was for the purpose of investigating potential fraud or misrepresentation'.[25] However, the ALRC considers that individuals or organisations that pursue such conduct—where it is reasonable and proportionate—will already be protected from liability given the operation of the public interest balancing test proposed in Chapter 8. In that chapter, the ALRC proposes that 'the prevention and detection of crime and fraud' be included in a list of public interest factors to be considered by a court.[26]

10.30 Furthermore, in some instances, the power to investigate fraudulent insurance claims is authorised by statute. For example, s 116 of the *Motor Vehicle Compensation Act 1999* (NSW) requires a licensed insurer to 'take all such steps as may be reasonable to deter and prevent the making of fraudulent claims'.

Reasonable, proportionate and necessary

10.31 The qualification that conduct be 'reasonable, proportionate and necessary' will provide a court with the opportunity to balance competing interests.[27] Privacy is a complex concept which necessarily involves analysis of competing interests and assessments of proportionality. The qualification that conduct be proportionate, necessary and reasonable acknowledges the fact that the circumstances leading to an invasion of privacy require careful consideration.

10.32 This balancing process is consistent with other elements of the cause of action, specifically the public interest test. Witzleb argued that requiring a balance of competing interests in the defence that conduct was incidental to the defence of person,

---

22 Balkin and Davis, above n 3, [6.17].
23 This defence is codified in some Australian jurisdictions, for example: *Criminal Code Act 1899* (Qld) s 274.
24 These were pursued under the *Privacy Act*, RSBC 1996, c 373 (British Columbia).
25 Insurance Council of Australia, *Submission 15*.
26 See, Proposal 8-2.
27 Law Institute of Victoria, *Submission 22*.

property or interests 'underlies the cause of action as a whole, in particular in relation to countervailing public interests'.[28]

10.33 The operation of this qualified defence relies on concepts of proportionality and reasonableness which are derived from human rights jurisprudence. Their inclusion in the new Act would make it more consistent with Australia's international human rights obligations to appropriately balance the protection of privacy with free speech and other interests.[29] The UN Human Rights Committee has stated that proportionality is a fundamental test which is necessary to justify any restriction on human rights under the ICCPR.[30]

10.34 Some stakeholders may argue that this qualified defence shifts the burden of proof from the question of whether there has been a serious invasion of privacy, to whether there has been a *justifiable* invasion. Any such emphasis would not prevent an equitable outcome. A defendant will be required to show that there was at least an apprehended threat to their privacy interest and that the invasion of privacy was necessary and reasonable for the protection of his or her rights against that threat.

10.35 The ABC submitted that the qualification of proportionality is 'appropriate' and consistent with media guidelines including their Editorial Policies and Code of Practices.[31]

Absolute privilege

Proposal 10–3 The new Act should provide for a defence of absolute privilege for publication of private information that is co-extensive with the defence of absolute privilege to defamation.

10.36 The ALRC proposes that the defence of absolute privilege be available as a defence to the new tort.[32] This defence should be stated to be co-extensive with the defence of absolute privilege to defamation, so that it includes both statutory and common law defences of absolute privilege.[33]

---

28 N Witzleb, *Submission 29*.

29 *International Covenant on Civil and Political Rights*, Opened for Signature 16 December 1966, UNTS 171 (entered into Force 23 March 1976) Articles 17, 19.

30 UN Human Rights Committee, General Comment No 29, U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001).

31 ABC, *Submission 46*.

32 The ALRC and the VLRC previously recommended of a defence of privilege to a statutory cause of action. Some stakeholders preferred the availability of a broad privilege defence: Office of the Australian Information Commissioner, *Submission 66*. The NSWLRC recommended the defence of absolute privilege, qualified privilege to protect a duty or interest, qualified privilege to protect the fair reporting of public proceedings and innocent dissemination. Several stakeholders supported the inclusion of this defence: Arts Law Centre of Australia, *Submission 43*; Law Institute of Victoria, above n 30; ABC, above n 1; Telstra, *Submission 45*; NSW Young Lawyers, above n 1; D Butler, *Submission 10*.

33 Eg *Defamation Act 2005* (SA) s 27; Des A Butler and Sharon Rodrick, *Australian Media Law* (Thomson Reuters (Professional) Australia Limited, 2011) 67. See also NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.9] and Draft Bill, cl 75.

10.37 Absolute privilege protects individuals who reveal personal information about another person in the course of public forums such as parliament and proceedings in a court or tribunal.[34] Publication on an occasion of absolute privilege provides a defendant with complete protection from liability in defamation. Rigorous debate in such proceedings may involve the revelation of personal information. Absolute privilege applies to statements made in these particular contexts in order to 'protect and facilitate frank and fearless communication even if it is damaging to reputations because it is considered in the public interest to do so'.[35]

10.38 In *Mann v O'Neill* a majority of the High Court of Australia stated that absolute privilege attaches to statements made in the course of parliamentary proceedings for reasons of inherent necessity or, as to judicial proceedings, as an indispensable attribute of the judicial process.[36] This defence operates as a function of Australia's democratic system by facilitating the free and fair exchange of debate in certain circumstances which may involve the disclosure of an individual's private information.

10.39 The defence is in addition to other forms of privilege such as parliamentary privilege which attaches to statements made within the confines of a parliamentary chamber to protect members of parliament (MPs) from liability.[37]

Qualified privilege

Proposal 10–4 The new Act should provide for a defence of qualified privilege to the publication of private information where the defendant published matter to a person (the recipient) in circumstances where:

(a) the defendant had an interest or duty (whether legal, social or moral) to provide information on a subject to the recipient; and

(b) the recipient had a corresponding interest or duty in having information on that subject; and

(c) the matter was published to the recipient in the course of giving to the recipient information on that subject.

The defence of qualified privilege should be defeated if the plaintiff proves that the conduct of the defendant was actuated by malice.

Question 10–1 Should the new Act instead provide that the defence of qualified privilege is co-extensive to the defence of qualified privilege to defamation at common law?

---

34 Legislation provides a non-exhaustive list of occasions which attract absolute privilege, for example, *Defamation Act 2005* (NSW) s 27. Schedule 1 of the uniform defamation laws extends absolute privilege to other occasions.

35 N Witzleb, *Submission 29*.

36 *Mann v O'Neill* [1997] HCA 28 (31 July 1997) 212 (Brennan CJ, Dawson, Toohey and Gaudron JJ).

37 *Parliamentary Privileges Act 1987* (Cth) s 16 and parallel state acts. See, Butler and Rodrick, above n 34, [3.700].

10.40 The ALRC is particularly interested in comments from stakeholders and legal practitioners as to the need for and practicability of a defence of qualified privilege for the publication of private information and the content of the defence.

10.41 This proposal is modelled on the proposal of the NSWLRC.[38]

10.42 There are three ways in which qualified privilege operates as a defence in defamation law. First, there is the defence at common law which operates on occasions of qualified privilege.[39]

> The common law protects a defamatory statement made on an occasion where one person has a duty or interest to make the statement and the recipient of the statement has a corresponding duty or interest to receive it. Communications made on such occasions are privileged because their making promotes the welfare of society. But the privilege is qualified - hence the name qualified privilege - by the condition that the occasion must not be used for some purpose or motive foreign to the duty or interest that protects the making of the statement.[40] (footnotes omitted)

10.43 The duty which the common law protects may be a legal, social or moral duty.[41] The reciprocity of interest or duty is essential, thus the common law defence tends to apply only to publications that are limited in extent to individuals or groups with a particular common interest. Matters which the court will consider in deciding whether the occasion was one of qualified privilege include 'the nature of the defamatory communication, the status or position of the publisher, the number of recipients and the nature of any interest they had in receiving it, and the time, place and manner of, and reason for, the publication'.[42]

10.44 The fact that a matter was one of public interest does not of itself attract qualified privilege. The common law defence is therefore of little utility to the media because of the usually wide extent of publication, except in very limited circumstances such as the publication of a reply to an attack or the correction of previously published information. It does however provide important protections for statements made without malice on limited occasions.

10.45 Secondly, there is the defence of qualified privilege under s 30 of the uniform defamation laws of 2005 (UDL).[43] This requires the publication to have been made where the recipient of the information had an interest or apparent interest in having information; the matter was published to the recipient in the course of giving that information to the recipient; and the defendant's conduct in publishing the matter was reasonable in the circumstances. The UDL sets out a number of considerations which

---

38 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009), [6.11]-[6.12].

39 *Toogood v Spyring* (1834) 1 CM & R 181; 149 ER 1044; *Australian Broadcasting Corporation v Comalco Ltd* (1986) 12 FCR 510; *Harbour Radio Pty Ltd v Trad* [2012] HCA 44; *Atkas v Westpac Banking Corporation Ltd* [2010] HCA 25.

40 *Roberts v Bass* (2002) 212 CLR 1, [62] (Gaudron, McHugh and Gummow JJ).

41 *Adam v Ward* [1917] AC 309, 334.

42 *Bashford v Information Australia (Newsletters) Pty Ltd* [2004] HCA 5 (2004) [54] (McHugh J).

43 See, *Defamation Act 2005* (NSW); *Defamation Act 2005* (SA); *Defamation Act 2005* (WA); *Defamation Act 2006* (NT) 2006; *Defamation Act 2005* (Qld) 2005; *Defamation Act 2005* (Vic); *Defamation Act 2005* (Tas).

the court may take into account when determining whether the conduct of the defendant was reasonable, including the extent to which the published matter is in the public interest, the seriousness of the matter, and the source of the information.

10.46 The statutory defence in the UDL is modelled on s 22 of the *Defamation Act 1974* (NSW)[44] but includes additional factors. Because of, among other things, its inclusion of public interest as a relevant consideration, the statutory defence is more useful to the media than common law qualified privilege, although it also requires proof that the defendant acted reasonably, which may not be a conclusion that courts will draw without convincing proof. Like the common law defence, the defence is defeated where the publication was actuated by malice.

10.47 Essentially the value to defendants of the statutory defence over the common law was that it could be used to defend publications in the public interest. The ALRC considers that a defence in similar terms to s 30 of the UDL is unnecessary in view of the balancing of public interest required for actionability of the cause of action.

10.48 The third type of qualified privilege defence is the extended common law defence of qualified privilege which encompasses the implied constitutional freedom of communication on government and political matters, as formulated by the High Court of Australia in *Lange v Australian Broadcasting Corporation.*[45] The defence is defeated where the publication was actuated by malice. Again, because of the public interest required for actionability of the cause of action, the ALRC considers that there is no need to make special provision for this freedom. An invasion of privacy would not be actionable where this would infringe or unduly burden the implied freedom of political communication.

10.49 The proposal is then a statutory formulation only of the defence of qualified privilege at common law. The defence may be useful where a publication made under a relevant duty or interest is not protected by absolute privilege, by the public interest consideration in the cause of action, or by the defence of lawful authority set out above.

10.50 Examples may include where an individual shares a mutual interest with the recipient, such as in a tenancy or building matter involving a common landlord or neighbour; where the individual and recipient are co-employees or co-members of an association; or where a defendant is subject to a legal duty which necessitates the disclosure of private information such as where an individual provides a statement to police containing a third party's private information[46] or informs a professional body about the health or conduct of a member. The NSWLRC gave the example of a person providing an employment reference.[47] Without a defence of qualified privilege, individuals would have to rely on broader defences which may provide inadequate protection.

---

44 Butler and Rodrick, above n 33, [3.1000–3.1050].

45 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *Attorney-General (SA) v Corporation of the City of Adelaide* [2013] HCA 3 (27 February 2013).

46 Law Institute of Victoria, *Submission 22*.

47 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.12].

10.51 There are a number of similar defences in state and territory surveillance devices legislation relating to communications which are reasonably necessary to protect a defendant's interest, to protect the public interest, and are made in the course of legal proceedings.[48] These may act as a guide for legislators. So too may the range of defamation defences available at US tort law. These were canvassed in D Butler's submission.[49] At US law, qualified or conditional privilege is also understood as common interest privilege and extends to the protection of an interest of the recipient of a defamatory matter, or a third person.[50] In *Indianapolis Horse Patrol, Inc. v. Ward* (1966), 247 Ind. 519, 524, 217 N.E.2d, the Indiana Supreme Court held that:

> The rule concerning a qualified privilege is that a communication made in good faith on any subject matter in which the party making the communication has an interest or in reference to which he has a duty either public or private, either legal, moral, or social, if made to a person having a corresponding interest or duty, is privileged.

10.52 Whilst supporting the defence of qualified privilege, SBS qualified this support by arguing that concepts of reasonableness and proportionality should affect the operation of the defence[51] and that guiding principles look at the conduct of the disclosing party (for example, was it reasonable? was it proportionate?). The ALRC has not included these particulars in its proposal, because the defence proposed is already limited by such factors.

Publication of public documents

Proposal 10–5 The new Act should provide for a defence of publication of public documents.

10.53 The defence should be similar in terms to the defence for publication of public documents in the UDL which attaches privilege to the publication of public documents including court judgements, and reports and papers tabled in Parliament, and Parliamentary voting records, where the copies are fair and accurate.[52] The ALRC considers the meaning of 'public documents' in defamation legislation would apply to this defence, though the ALRC leaves this task to drafters.

10.54 Access to public documents supports a transparent and open government and judicial system. This proposal is consistent with the ALRC's Terms of Reference for this Inquiry which requires consideration of the effect of a cause of action on the necessity of balancing privacy with fundamental values including freedom of expression and open justice.

10.55 The NSWLRC argued that the consideration of public interest in their recommended statutory cause of action provided adequate protection for publication of

---

48 Eg *Surveillance Devices Act 2007* (NSW) s 11(2); *Surveillance Devices Act 1998* (WA) s 9(2).
49 D Butler, *Submission 10*.
50 American Law Institute, *Restatement of the Law Second, Torts* (1977) §§ 595, 596.
51 SBS, *Submission 59*.
52 *Defamation Act 2005* (SA) s 28.

public documents and fair report of proceedings of public concern.[53] A number of media stakeholders expressed their support for the availability of this defence.[54]

Fair report of proceedings of public concern

Proposal 10–6 The new Act should provide for a defence of fair report of proceedings of public concern.

10.56 This proposal provides a defence for individuals who fairly report on public proceedings which may reveal private information that could otherwise amount to a serious invasion of privacy. This defence will be of particular significance to media organisations, court reporters and educational institutions.

10.57 The provision is modelled on the defence of fair report of proceedings of public concern in the UDL.[55] This statutory defence to defamation applies to the publication of defamatory matter contained in documents from public proceedings such as proceedings of a Parliamentary body, an international organisation, court or tribunal, inquiries including Royal Commissions, meeting of shareholders of a public company, and other public proceedings.

10.58 The ALRC considers that the meaning of 'fair' as it has developed at common law and in the interpretation of defamation statutes should apply to this proposal. In that context, *fair* refers to summaries of proceedings which intend to honestly convey to the reader the impression which the proceedings would have had.[56] Whether a report is fair will be a question of fact for a court.

Necessity

Question 10–2 Should the new Act provide for a defence of necessity?

10.59 The ALRC is not proposing a defence of necessity at this stage in the Inquiry, however the ALRC welcomes stakeholder responses to the question raised in this section.

10.60 A defence of necessity would protect individuals from liability where a situation of overwhelming urgency justifies a serious invasion of privacy.[57] This defence will arise in situations where a defendant is or feels compelled[58] to invade an individual's

---

53 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.8].

54 SBS, *Submission 59*; D Butler, *Submission 10*.

55 *Defamation Act 2005* (SA) s 29.

56 *Cook v Alexander* [1974] 1 QB 279 [288]; *Bashford v Information Australia (Newsletters) Pty Ltd* [2004] HCA 5 (2004); *Rogers v Nationwide News Pty Ltd* (2003) 201 ALR 184.

57 Telstra suggested the availability of an exemption for emergency services: Telstra, *Submission 45*. T Gardner, *Submission 3* was in favour of a defence of necessity.

58 The defence of necessity to intentional torts involves an assessment by the court that the steps taken by an individual to prevent imminent danger were reasonable. See, Balkin and Davis, above n 3, [6.21].

privacy in order to prevent or reduce the occurrence of a more serious harm. Situations of public emergency where emergency service professionals need to access the private information of at-risk or vulnerable persons may give rise to this defence. This necessity may arise for example, where an individual has indicated an intention to commit suicide and mental health professionals or emergency services require private information from another individual. Or where a doctor is called to a school and needs to reveal private information about vaccinations or a contagious disease or condition.[59]

10.61 The defence of necessity is an established defence to intentional torts to protect activities and conduct pursued to prevent a greater harm,[60] including in medical and other emergencies, and is recognised in criminal law.[61]

10.62 This defence differs from qualified privilege as it does not involve a mutual interest between two parties which necessitates the disclosure of private information or intrusion into someone's seclusion. Moreover, a defence of necessity provides more targeted protection than is offered by the public interest test as arguably public interest focuses on invasions carried out in the interests of public or community safety and wellbeing rather than that of an individual or smaller group. While there may be some overlap in defences, the ALRC does not consider this a problem.

Safe harbour scheme for internet intermediaries

Proposal 10–7 The new Act should provide a safe harbour scheme to protect internet intermediaries from liability for serious invasions of privacy committed by third party users of their service.

Question 10–3 What conditions should internet intermediaries be required to meet in order to rely on this safe harbour scheme?

10.63 The ALRC proposes the introduction of a safe harbour scheme for internet intermediaries,[62] to protect them from liability for serious invasions of privacy committed by persons who use their services,[63] where the intermediary meets certain conditions. Where an intermediary meets these conditions, a plaintiff will only be able to pursue the third party, the primary tortfeasor. This defence will not apply to invasions of privacy that intermediaries themselves intentionally commit.

---

59 News Limited, Special Broadcasting Service, Submission No 76 to DPM&C Issues Paper, 2011.

60 Balkin and Davis, above n 3, [6.21].

61 *R v Loughnan* [1981] VR 443, [448].

62 The broad term 'internet intermediary' is commonly used to cover: carriage service providers, such as Telstra or Optus; content hosts, such as Google or Yahoo!; and search service and application service providers, such as Facebook, Flickr and YouTube: Peter Leonard, 'Safe Harbors in Choppy Waters-Building a Sensible Approach to Liability of Internet Intermediaries in Australia' (2010) 3 *Journal of International Media and Entertainment Law* 221, 226.

63 A safe harbour exemption was recommended by some stakeholders in response to the DPM&C's 2011 Issues Paper: Peter Leonard and Michael Burnett, Submission No 77 to DPM&C Issues Paper, 2011.

10.64 Special defences for internet intermediaries may be necessary for a number of reasons. Imposing liability on internet intermediaries for serious invasions of privacy by third parties may impose onerous obligations on platforms to review and moderate user-generated content. Given the quantity of material generated on these sites, and the instantaneous way in which online communications are sent and received, this may be oppressive and unreasonable. Facebook submitted that the cost to online businesses of reviewing third party content before it appears on their platforms would be prohibitive.[64]

10.65 While software may be used to detect pornography, using software to identify content that invades someone's privacy may be more difficult. Peter Leonard has written that 'such fact-based determinations require contextual analysis and, in many instances, additional facts'.[65]

10.66 Safe harbours are used in various contexts at Australian law including in classification and copyright law.[66] For instance, the *Broadcasting Services Act* 1992 (Cth) provides immunity for online content platforms where the host was not aware of the nature of the relevant content.[67] Online content platforms must show a lack of awareness or knowledge of the offending content hosted on their site in order to access this provision.

10.67 There are comparable safe harbours at US and European law.[68] Section 230 of *Communications Decency Act 1996* (US) contains a particularly strong and broadly applicable[69] safe harbour scheme:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider...No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.[70]

10.68 Section 230 has been said to have 'flourished' in the United States.

> It has been interpreted quite broadly to apply to any form of Internet intermediary, including employers or other companies who are not in the business of providing Internet access and even to individuals who post the content of another. And it has been uniformly held to create absolute immunity from liability for anyone who is not the author of the disputed content, even after they are made aware of the illegality of the posted material and even if they fail or refuse to remove it. The result is that Internet intermediaries need not worry about the legality of the content others post or

---

64 Facebook, Submission 65.

65 Leonard, above n 62, 238.

66 *Copyright Act 1968* (Cth) s 116AG.

67 *Broadcasting Services Act 1992* (Cth) sch 5 cl 91.

68 *Communications Decency Act 1996, Title V of the Telecommunications Act 1996, 47 U.S.C*; *EU Directive on Electronic Commerce (2000/31/EC)*. Articles 14 and 15 of the EU directive protect certain 'information society service providers' from liability for damages or other pecuniary remedy or any criminal sanction, though not from injunctive relief, in circumstances where information was disclosed with their knowledge or control.

69 M Lemley, 'Rationalizing Internet Safe Harbors' (2007) 6 *J. on Telecomm. & High Tech. L.* 101, 102.

70 *Communications Decency Act 1996,* Title V of the *Telecommunications Act 1996,* 47 U.S.C.

> send through their system, with one significant exception: section 230 does not apply to intellectual property claims.[71]

10.69 Electronic Frontiers Australia supported the adoption in Australia of a model similar section 230.[72]

10.70 In the US case of *Barnes v Yahoo!,*[73] a woman unsuccessfully sued Yahoo! for its failure to remove compromising photographs of her—posted by a third party—from a Yahoo! message board which a Yahoo! employee had agreed to remove from its website. The US court of Appeals for the Ninth Circuit ruled that Yahoo! could not be sued in tort for invasion of privacy[74] because of the operation of s 230 of the *Communications Decency Act*:[75] a website cannot be treated as the 'publisher or speaker' of material posted online by a third party.

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

10.72 Similarly, the UK's *Defamation Act 2013* provides a defence for 'Operators of websites'.[76] The defence will be defeated if a claimant proves that: it was not possible for the claimant to identify the person who posted the statement; the claimant gave the operator a notice of complaint in relation to the statement; and the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations. Given the proposal of a safe harbour exemption for internet intermediaries, the ALRC has not proposed a defence of innocent dissemination.

10.73 The defence of innocent dissemination may be considered a type of safe harbour.[77] Innocent dissemination is a defence to the publication of defamatory matter, available where a defendant proves that they published the defamatory material merely in the capacity of a 'subordinate distributor'. This means that they neither knew, nor ought reasonably to have known, that the matter was defamatory, and that their lack of knowledge was not due to any negligence.[78] As noted above, a number of stakeholders submitted that there should be a defence of innocent dissemination to any new Australian cause of action for serious invasion of privacy.

10.74 However, unlike the safe harbour scheme proposed above, a defence of innocent dissemination does not impose any additional conditions on the defendant. The ALRC considers that such additional conditions may be justified.

---

71 Lemley, above n 69, 103.
72 Electronic Frontiers Australia, *Submission 44*.
73 *Barnes v Yahoo!, Inc 570 F3d 1096 (9th Circ 2009)*.
74 Paul J Larkin, '"Revenge Porn", State Law and Free Speech' (2014) 48 *Loyola of Los Angeles Law Review* (forthcoming).
75 *Communications Decency Act 1996,* Title V of the *Telecommunications Act 1996,* 47 U.S.C.
76 *Defamation Act 2003* (UK) 2013 s 5.
77 Leonard, above n 62, 235.
78 Eg *Defamation Act 2005* (NSW) s 32.

10.75 A safe harbour scheme may not be necessary if, as the ALRC proposes, the new tort is only actionable where the defendant has *intentionally or recklessly* invaded the privacy of the plaintiff. Internet intermediaries may rarely have this requisite fault when third parties use their services to invade someone's privacy.

10.76 However, argument may be raised as to whether they would be liable in some circumstances, for example, perhaps when given notice of a serious invasion of privacy that they have the power to prevent. The ALRC proposes the enactment of a safe harbour scheme to avoid doubt and provide the necessary certainty to internet intermediaries.

Conditions

10.77 To rely on a safe harbour defence, internet intermediaries might be required to comply with certain conditions. For example, they might be required to do some or all of the following:

- remove, or take reasonable steps to remove, material that invades a person's privacy, when given notice;
- provide consumer privacy education or awareness functions, such as warnings about the risk of posting private information;
- comply with relevant industry codes and obligations under the *Privacy Act 1988* (Cth);
- provide individuals with a mechanism to remove private content they post on online platforms; and
- provide a privacy complaints system where the intermediary responds in a reasonable time to consumer complainants.

10.78 The ALRC is interested in stakeholder views on what conditions should be imposed on internet intermediaries, in order for them to be able to rely on a safe harbour defence to serious invasions of privacy.

Unnecessary defences

Other defamation defences

10.79 The ALRC is not proposing that all defences to defamation be replicated in the new tort. There are differences in the nature and application of the two causes of action which mean that not all defamation defences are appropriate in a privacy context.

10.80 First, the defence of truth is not relevant to a privacy tort. Most cases involving invasions of privacy by disclosure of information are brought to prevent or seek redress for disclosure of true information.

10.81 Secondly, a defence of fair comment as in defamation law[79] is arguably inappropriate for a privacy tort. Public interest will already have been considered as

79 The *Privacy Act*, RSBC 1996, c 373 s 2 includes the defence of fair comment.

part of the actionability of the cause of action, so that a defence is unnecessary: the right to speak freely that is protected by the defence of fair comment in defamation law, both at common law and under the UDL, is limited to matters of public interest. Further, the relevant wrong in the invasion of privacy tort is the disclosure of information. Outside matters of public interest, a person should not be able to disclose private information about another under the guise of making a comment or opinion.[80] The VLRC recommended a defence of fair comment but such a defence was not recommended by the ALRC previously or by the NSWLRC.[81]

10.82 Thirdly, the defence of innocent dissemination[82] is inappropriate, as the statutory cause of action is limited to intentional acts. In any event, the ALRC has proposed a safe harbour scheme, which may provide a suitable defence for some innocent disseminators of material that invades privacy.

10.83 Lastly, the defence of triviality is unnecessary as the statutory cause of action is confined to *serious* invasions of privacy.[83]

Material in the public domain

10.84 Several stakeholders supported the inclusion of a defence that the material was already in the public domain.[84] However the ALRC proposes that consideration of whether and to what extent material was in the public domain should be considered by a court when determining whether a plaintiff had a reasonable expectation of privacy.[85] This factor is therefore discussed more fully in Chapter 6. The ALRC recognises that there may be some circumstances where the widespread dissemination of an individual's private information may diminish their reasonable expectation of privacy. However a complete defence would be inappropriate as the extent and effect of a prior disclosure on an individual's privacy is variable. Moreover, unlike confidential information, private information does not necessarily lose its quality of privacy once it has been disclosed. PIAC argued that information may still be private in nature, despite the fact that it has been published.[86] Information such as a person's criminal record, certain health information such as their HIV status, or the fact that they were a victim of crime may no longer be of such public interest that publication outweighs the reasonable expectation of privacy.

Public interest

10.85 The ALRC has proposed earlier in this Discussion Paper that a plaintiff only has a cause of action for serious invasion of privacy where a court is satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of

---

80 N Witzleb, *Submission 29*.

81 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.8].

82 Some stakeholders supported the inclusion of a defence of innocent dissemination, eg, Office of the Australian Information Commissioner, *Submission 66*; SBS, *Submission 59*. However the necessity of the defence flows from the fault element of the cause of action.

83 SBS, above n 21 supported the availability of the defence of triviality.

84 Ibid; ABC, *Submission 46*; D Butler, *Submission 10*; T Gardner, *Submission 3*.

85 N Witzleb, *Submission 29*.

86 Public Interest Advocacy Centre, *Submission 30*.

expression and any broader public interest.[87] A defence of public interest is therefore unnecessary. Public interest is discussed more fully in Chapter 8.

10.86 Several stakeholders favoured a defence of public interest.[88] Some stakeholders argued that a defence would provide greater accessibility to litigation for plaintiffs as defendants will often be in a better position to adduce evidence relevant to the question of whether there was a public interest in their conduct.[89] In the case of a media organisation for instance, this may be due to their experience in handling public interest similar matters such as submitting FOI requests to government agencies in the public interest.

10.87 Similar or analogous actions also provide for a public interest defence. For instance, qualified privilege under the UDL[90] provides that a court may consider public interest matters when assessing whether a defendant behaved reasonably when publishing a defamatory matter.

10.88 However, the ALRC considers that a balancing exercise is a more appropriate way to determine whether there is a public interest in the disclosure of the private information or the intrusion into an individual's seclusion. Expressly incorporating public interest into the actionability of a statutory cause of action will ensure that privacy interests are not unduly privileged over other rights and interests, particularly given that Australia does not have express human rights law protection for freedom of speech.

Consent

10.89 Several stakeholders argued in favour of a defence of consent.[91] The ALRC proposes that whether the plaintiff has consented to the conduct of the defendant should be considered as a factor in whether the plaintiff had a reasonable expectation of privacy. The inclusion of consent in the test for actionability will provide an opportunity for the court to balance the quality and scope of a plaintiff's consent with the defendant's conduct and interests.

Contributory negligence

10.90 The ALRC is not proposing a defence of contributory negligence. A defence of contributory negligence would have the effect of defeating a claim for serious invasion

---

87 Several stakeholders supported this model: Office of the Australian Information Commissioner, *Submission 66*; Google, *Submission 54*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*.

88 NSW Young Lawyers, *Submission 58*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; Pirate Party of Australia, *Submission 18*; Law Institute of Victoria, *Submission 22*; D Butler, *Submission 10*; T Gardner, *Submission 3*.

89 Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; D Butler, *Submission 10*.

90 *Defamation Act 2005* (SA) s 30.

91 Google, *Submission 54*; Australian Communications and Media Authority, *Submission 52*; ABC, *Submission 46*; Interactive Games and Entertainment Association, *Submission 40*; Australian Privacy Foundation, *Submission 39*; I Turnbull, *Submission 5*.

of privacy where a plaintiff's failure to take reasonable care contributed to the invasion of their privacy. Further, because contributory negligence is not to be a defence, there would also be no basis for arguing that the apportionment provisions in state and territory legislation[92] should apply.

10.91 A defence of contributory negligence would be inconsistent with the design of the cause of action which is limited to intentional conduct. The ALRC considers that where a defendant intends to invade another person's privacy, and cannot rely on one of the available defences, that conduct should not be excused or mitigated by any fault of the plaintiff. This approach is consistent with the law relating to other intentional torts law, such as conversion, battery and assault.[93]

Other defences and exemptions

10.92 Several stakeholders expressed the view that no activity or organisation should be exempt from the statutory cause of action, arguing that defences would be sufficient to protect serious invasions of privacy which are nonetheless warranted.[94]

10.93 Stakeholders have raised a number of other possible exemptions and defences. However, the ALRC considers that many of these are appropriately captured by the defences proposed above. SBS favoured an exemption for journalists and media organisations, provided the serious invasion of privacy occurs whilst they are engaged in journalism.[95] This would operate in a similar fashion to the journalism exemption in the *Privacy Act* 1988 (Cth).

10.94 Telstra favoured an emergency services exemption.[96] The Australian Bureau of Statistics (ABS) favoured an exemption for the use of official data for statistical and related purposes.[97] The Australian Bankers' Association argued that compliance with the *Privacy Act 1988* (Cth) should be a complete exemption to a statutory cause of action for serious invasion of privacy.[98]

10.95 Voiceless and the Barrister's Animal Welfare Panel Ltd submitted that there should be a defence for activities carried out 'for the purpose of, or resulted in, the procuring of evidence of an iniquity'.[99] The ALRC considers that such a defence would be much too extensive. The defence of lawful authority and the defence for conduct incidental to the exercise of a lawful right of defence of persons or property, both proposed above, are more appropriate.

---

92 Eg *Law Reform (Miscellaneous Provisions) Act 1956* (NT); *Personal Injuries (Liabilities and Damages) Act* (NT); *Civil Liability Act 2003* (Qld).

93 Cf *New South Wales v Riley* (2003) 57 NSWLR 496, [104].

94 Office of the Australian Information Commissioner, Submission 66; Law Society of NSW Young Lawyers Communications, Entertainment and Technology Committee and Human Rights Committee, Submission 58; Queensland Council of Civil Liberties, Submission 51; ABC, Submission 46; Australian Privacy Foundation, Submission 39; N Witzleb, Submission 29; Law Institute of Victoria, Submission 22.

95 SBS, *Submission 59*.

96 Telstra, *Submission 45*.

97 Australian Bureau of Statistics, *Submission 32*.

98 Australian Bankers' Association, *Submission 27*.

99 Barristers Animal Welfare Panel and Voiceless, *Submission 64*.

10.96 The Arts Law Centre of Australia[100] (supported by the National Association for the Visual Arts and the Australian Institute of Professional Photography) favoured the following exemptions: photography or filming in a public place; documentary film-making or photography; journalistic or investigative photography, film-making or reporting; photography or filming of privately owned land or premises, or people on those premises, where the premises are accessible to the public; and photography or filming of people on private premises for purposes such as education, journalism, artistic expression and documentary.

100 Arts Law Centre of Australia, *Submission 43*.

11. Remedies and Costs

Contents

Summary

11.1 The ALRC proposes that courts be granted the discretion to award a range of remedies—monetary and non-monetary—to plaintiffs who successfully bring an action for serious invasion of privacy.

11.2 The proposed range of remedies reflects the different objectives, experience and circumstances of plaintiffs who may pursue privacy actions. Some plaintiffs may seek monetary compensation, some may wish the offending behaviour to cease, some will seek to deter similar conduct in the future, while others may seek public vindication of their interests. A range of non-monetary remedies may provide a more appropriate response for the often immeasurable effects occasioned by invasions of privacy.

11.3 Most actions for invasion of privacy will concern harm to dignitary interests or emotional distress. It is therefore important that courts may award compensatory damages, including damages for the plaintiff's emotional distress, in an action for serious invasion of privacy.

11.4 This chapter begins with the ALRC's proposal for the courts to be empowered to award damages for economic and non-economic loss, including damages for any emotional distress suffered by the plaintiff. The ALRC proposes that a court may consider a range of mitigating and aggravating factors in the assessment of such damages, and that a separate award of aggravated damages may not be made. A court

should have the discretion to award exemplary damages in exceptional circumstances where the court considers that other damages would not be a sufficient deterrent against such conduct occurring in the future. The total award of damages available for exemplary damages and damages for non-economic loss should be capped at the same level as damages for non-economic loss in defamation. This will avoid plaintiffs cherry-picking between defamation and privacy.

11.5 The ALRC also proposes that a court be empowered to award an account of profit in circumstances where a defendant has profited from the invasion of privacy. A court should be empowered to assess damages by reference to a notional licence fee.

11.6 The ALRC also proposes that courts be empowered to award non-monetary remedies: injunctive relief; an order requiring the defendant to apologise; a correction order; an order for the delivery up, destruction or removal of material; and declaratory relief. These remedies are not mutually exclusive, and may also be awarded in addition to monetary remedies. It will be at the discretion of a court to award appropriate relief in all the circumstances of a case. Therefore, a non-monetary order such as injunctive or declaratory relief will not necessarily reduce an award of damages.

Compensatory damages

Proposal 11–1 The new Act should provide that courts may award compensatory damages, including damages for the plaintiff's emotional distress, in an action for serious invasion of privacy.

11.7 The ALRC proposes that courts be empowered to award compensatory damages for loss suffered to a plaintiff, including damages for emotional distress. Previous law reform inquiries made similar recommendations.[1]

11.8 Compensatory damages would be assessed by reference to existing tort principles.[2] One reason for the ALRC's proposal that the statutory cause of action be described as an action in tort[3] is to allow a court when determining an action for serious invasion of privacy to draw on principles that have been well settled and applied by the courts in analogous common law actions. The proposal that the new tort be actionable per se will make it most closely analogous to actions like trespass to the person, but it will also be analogous in other respects to defamation actions.

1 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) cl 76(1)(a); Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) Rec 29(a).

2 K Barker et al, *The Law of Torts in Australia* (Oxford University Press, 2012) chs 2.8, 16.

3 See Ch 4.

11.9 It should first be noted that nominal damages would not be appropriate in an action for *serious* invasion of privacy.[4]

11.10 A plaintiff might suffer actual loss in the form of physical or psychiatric injury, property damage[5] or other economic loss as a result of the serious invasion of privacy. Regardless of the type of harm or the tort, the general principle in tort law is that the role of compensatory damages is to place a plaintiff, so far as money can do, in the position he or she would have been in had the tort not been committed.[6]

11.11 Where a plaintiff has suffered physical or psychological injury, compensatory damages may include special[7] and general[8] damages to remedy economic loss suffered by a plaintiff, as well as general damages for non-economic loss. The financial loss suffered by a plaintiff may include medical expenses incurred and loss of earnings as a result of the injury and in some instances, the effect of the injury on a plaintiff's future earnings.[9] Damages for non-pecuniary loss recognise the pain and suffering caused by the injury.

11.12 However, the ALRC proposes that the new Act also clearly provide that a court may award damages for 'mere' emotional distress, in an action for serious invasion of privacy. Serious invasions of privacy commonly cause emotional distress or harm to the plaintiff's dignitary interests, often unaccompanied by any physical or psychiatric illness. This fact, given the failure of the common law to provide redress for the intentional infliction of mere emotional distress outside actions such as trespass, is one of the key justifications for the proposed statutory cause of action. So too is the uncertainty about whether Australian courts can award damages for emotional distress in equitable actions for breach of confidence.[10] Making an intentional or reckless serious invasion of privacy actionable per se will allow a court to award general damages in compensation for a plaintiff's emotional distress.

11.13 Compensation for distress or injury is not the only basis for an award of damages. In torts which are actionable per se, such as trespass to the person in the form of battery, assault or false imprisonment, trespass to land, and also in defamation where harm to the plaintiff's reputation from a defamatory statement is presumed,[11] the courts

---

4 Nominal damages are available in trespass cases: RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [27.3].

5 For example, damage to stock or the cost of repairs to property occasioned by trespass to land or trespass to goods: Ibid [5.15].

6 *Livingstone v Rawyards Coal Co* (1880) 5 App Cas 25, 39 (Lord Blackburn); *Harriton v Stephens* (2006) 226 CLR 52 [166] (Hayne J); *Butler v Egg Pulp Marketing Board* (1966) 114 CLR 185, 191 (Taylor and Owen JJ).

7 Special damages refer to 'those items of loss which the plaintiff has suffered prior to the date of trial and which are capable of precise arithmetical calculation—such as hospital expenses': Balkin and Davis, above n 4, [27.5].

8 General damages refer to all injuries which are not capable of precise calculation. They refer to financial loss which may be suffered after the date of judgement and all non-financial such as pain and suffering or loss of amenities: Ibid.

9 Ibid [11.27].

10 The only Australian appellate authority on the award of damages for emotional distress in a breach of confidence case is *Giller v Procopets* (2008) 24 VR 1. See Ch 12 for further discussion.

11 Balkin and Davis, above n 4, [18.17].

have often recognised that an award of general compensatory damages may serve the purpose or have the effect of vindicating the plaintiff's right. For instance, In *Uren v John Fairfax & Sons Pty Ltd* [1966], Windeyer J gave the following explanation of the purpose of compensatory damages in defamation:

> compensation by damages operates in two ways—as a vindication of the plaintiff to the public and as consolation to him for a wrong done.[12]

11.14 In *Plenty v Dillon* (1991), Gaudron and McHugh JJ of the High Court of Australia characterised the award of general damages for an action in trespass to land as fulfilling vindicatory purposes:

> the appellant is entitled to have his right of property vindicated by a substantial award of damages.[13]

11.15 Witzleb and Carroll explain that civil remedies are aimed at 'vindicating the interests that underlie the right or rights infringed'.[14]

Factors in mitigation and aggravation of general damages

Proposal 11–2 The new Act should set out the following non-exhaustive list of factors that may mitigate damages for serious invasion of privacy:

(a) that the defendant has made an appropriate apology to the plaintiff about the conduct that invaded the plaintiff's privacy;

(b) that the defendant has published a correction of any untrue information disclosed about the plaintiff;

(c) that the defendant has made an offer of amends in relation to the defendant's conduct or the harm suffered by the plaintiff;

(d) that the plaintiff has already recovered compensation, or has agreed to receive compensation in relation to the conduct of the defendant;

(e) that the defendant had taken reasonable steps to settle the dispute with the plaintiff in order to avoid the need for litigation; and

(f) that the plaintiff had not taken reasonable steps to settle the dispute, prior to commencing or continuing proceedings, with the defendant in order to avoid the need for litigation.

12 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 150 (Windeyer J).

13 *Plenty v Dillon* (1991) 171 CLR 635, 655.

14 Robyn Carroll and Normann Witzleb, '"It"s Not Just about the Money': Enhancing the Vindicatory Effect of Private Law Remedies' (2011) 37 *Monash University Law Review* 216, 219.

Proposal 11–3 The new Act should set out the following non-exhaustive list of factors that may aggravate damages for serious invasion of privacy:

(a) that the plaintiff had taken reasonable steps, prior to commencing or continuing proceedings, to settle the dispute with the defendant in order to avoid the need for litigation;

(b) that the defendant had not taken reasonable steps to settle the dispute with the plaintiff in order to avoid the need for litigation;

(c) that the defendant's unreasonable conduct at the time of the invasion of privacy or prior to or during the proceedings had subjected the plaintiff to special or additional embarrassment, harm, distress or humiliation;

(d) that the defendant's conduct was malicious or committed with the intention to cause embarrassment, harm, distress or humiliation to the plaintiff; and

(e) that the defendant has disclosed information about the plaintiff which the defendant knew to be false or did not honestly believe to be true.

11.16 The ALRC proposes that in assessing damages in an action for serious invasion of privacy, a court may consider any mitigating or aggravating factors which occurred before and during court proceedings.[15]

11.17 Mitigating factors have the effect of reducing the effect or the harm of the serious invasion of privacy and will therefore reduce the amount of compensatory damages awarded to a plaintiff. Aggravating factors such as whether the plaintiff suffered particular embarrassment or humiliation due to the nature of the defendant's conduct will increase the award of general damages.

11.18 Possible mitigating factors that a court may consider include whether either party had made attempts at alternative dispute resolution (ADR); whether the complaint had first been the subject of a determination by the Office of the Australian Information Commissioner, the ACMA or another body, (either by way of complaint or own-motion investigation) and the outcome of any determination; and whether a defendant had taken reasonable steps to redress the invasion of privacy such as through a public apology, correction order or removing the private information from an online platform.

11.19 Aggravating factors a court may consider include: where the defendant's conduct subjected a plaintiff to additional embarrassment or hurt; where their conduct

15 The *Defamation Act 2005* (NSW) s 38 sets out mitigating factors for a court when assessing damages. These include whether the defendant has made an apology to the plaintiff or has published a correction of the defamatory matter. In the tort of false imprisonment, the defendant's conduct up to and including conduct at the trial is relevant in a court's assessment of general and aggravated damages: *Spautz v Butterworth* (1996) 41 NSWLR 1.

was unjustifiable or improper;[16] or whether the defendant had published information which the defendant knew to be false.[17]

11.20 This proposal is also intended to encourage the parties to attempt to resolve their dispute without litigation if it would be reasonable to expect them to do so.

No separate award of aggravated damages

Proposal 11–4 The new Act should provide that the court may not award a separate sum as aggravated damages.

11.21 Given that the court is able to take into account any aggravating factors in the assessment of general damages, the ALRC proposes that the new Act should specifically provide that the court is not to make a separate award for aggravated damages.

11.22 At common law, aggravated damages are compensatory in nature as a form of general damages.[18] Aggravated damages comprise an additional sum to take account of the special humiliation suffered by the plaintiff due to the nature of the defendant's conduct in the commission of a wrong.[19] When considering such awards, courts have been astute to prevent the risk of damages overlapping in two ways. First, there is a potential for overlap between an ordinary award of general damages for injury to the plaintiff's feelings and an award of aggravated damages. Sackville AJA has noted that:

> In *New South Wales v Riley*, Hodgson JA (with whom Sheller JA and Nicholas J agreed) pointed out that in certain circumstances *"ordinary compensatory damages*" can be awarded for injury to feelings, falling short of a recognised psychiatric injury. Such damages can be awarded in actions for assault. His Honour also pointed out that, if, in addition to ordinary damages for injury to feelings, aggravated damages are to be awarded, it is important to avoid double counting. [20]

11.23 Secondly, there is a risk of overlap between the award for aggravated damages and that for exemplary damages, considered below, which are intended to punish or deter the defendant because of the nature of his or her conduct. As Spigelman CJ noted in *NSW v Ibbett*[21] in a passage approved by the High Court on appeal, 'in the case of aggravated damages the assessment is made from the point of view of the plaintiff and in the case of exemplary damages the focus is on the conduct of the defendant'.[22] Nevertheless, both awards have some reference to the nature of the defendant's

16 These standards have been applied by courts in NSW in assessing awards of aggravating damages; see, for example, *Mirror Newspapers Ltd v Fitzpatrick* (1984) 1 NSWLR 643, [653] (Samuels JA).
17 *McKenzie v Mergen Holdings Pty Ltd* (1992) 20 NSWLR 42, [361] (Grove J).
18 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 129–130 (Taylor J).
19 '[A]ggravated damages are given to compensate the plaintiff when the harm done to him by a wrongful act was aggravated by the manner in which the act was done': Ibid 149 (Windeyer J).
20 *New South Wales v Riley* (2003) 57 NSWLR 496, [129]. This passage was quoted by Sackville AJA in *New South Wales v Radford* [2010] NSWCA 276 (28 October 2010) [96].
21 *NSW v Ibbett* (2005) 65 NSWLR 168.
22 Ibid [83].

conduct. As Taylor J said in *Uren v John Fairfax & Sons Pty Ltd*, 'in many cases, the same set of circumstances might well justify either an award of exemplary or aggravated damages'.[23] This proposal will avoid the risk of both types of overlaps.

11.24 The ALRC's proposal is consistent with the approach of the NSWLRC on this issue. The NSWLRC explained that aggravating circumstances would already form some part of an assessment for general damages, stating that:

> To the extent to which the conduct of the defendant has increased the damage to the plaintiff, the plaintiff's loss is simply the greater—a fact that will, obviously, be reflected in the size of the award.[24]

Exemplary damages

Proposal 11–5 The new Act should provide that, in an action for serious invasion of privacy, courts may award exemplary damages in exceptional circumstances and where the court considers that other damages awarded would be an insufficient deterrent.

11.25 The ALRC proposes that a court be given the discretion to award exemplary damages in exceptional circumstances.[25] This head of damages focuses on the defendant's conduct rather than the plaintiff's loss. It may be appropriate where the defendant's conduct was in outrageous and contumelious disregard of the plaintiff's rights. An award of exemplary damages is intended to punish a defendant and deter similar conduct in the future.

11.26 The ALRC considers that the award of exemplary damages should only be made in exceptional circumstances or, in exceptional circumstances where the court is satisfied that the other damages or remedy awarded would not provide a sufficient deterrent against such conduct in the future. This later formulation would stress the arguably more valuable deterrent function of exemplary damages, rather than their punitive function.

11.27 The ALRC considers that a court should be able to make such an award, in exceptional circumstances, in an action under the proposed tort—particularly given that the tort proposed in this paper is confined to invasions of privacy that are both serious and intentional or reckless.[26] An award for exemplary damages is considered separately to other heads of damages.[27]

---

23 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 129–130 (Taylor J).

24 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [7.10].

25 Australian Privacy Foundation, *Submission 39*; Law Institute of Victoria, *Submission 22*; Women's Legal Centre (ACT & Region) Inc., *Submission 19*; I Turnbull, *Submission 5*; P Wragg, *Submission 4*; T Gardner, *Submission 3*.

26 See Chs 5 and 7.

27 *Henry v Thompson* (1989) 2 Qd R 412.

11.28 In *Lamb v Cotogno*[28] the High Court quoted from *Mayne & McGregor on Damages* their oft-cited description of exemplary damages:

> Such damages are variously called punitive damages, vindictive damages, exemplary damages, and even retributory damages. They can apply only where the conduct of the defendant merits punishment, which is only considered to be so where his conduct is wanton, as where it discloses fraud, malice, violence, cruelty, insolence or the like, or, as it is sometimes put, where he acts in contumelious disregard of the plaintiff's rights.[29]

11.29 Brennan J has said that an award of exemplary damages 'is intended to punish the defendant for conduct showing a conscious and contumelious disregard for the plaintiff's rights and to deter him from committing like conduct again'.[30]

11.30 While compensatory damages may often be sufficient remedy for serious invasions of privacy, additional damages will sometimes be justified where the conduct of the defendant can be characterised as outrageous or contumelious. Posting on the internet so-called 'revenge pornography'—intimate photographs or video of an ex-partner or ex-spouse without their consent—may be an example of an outrageous invasion of privacy.

11.31 Profits made from an invasion of privacy can be greater than the sum that is likely to be awarded to compensate the victim. Exemplary damages may help deter invasions of privacy that might otherwise be profitable for the defendant.

11.32 Furthermore, an award of exemplary damages may be more appropriate where a gain-based remedy is unavailable, such as in circumstances where a defendant had *attempted* to procure some financial gain from the intentional invasion of privacy but did not in fact make a profit.[31]

11.33 Although exemplary damages are available in Australia at common law for a wide range of intentional torts,[32] statute prevents the courts awarding exemplary damages in defamation claims.[33] They are also not available for breach of equitable obligations such as breach of confidence,[34] or in actions for breach of a contractual duty of confidence.[35]

---

28 *Lamb v Cotogno* (1987) 164 CLR 1, [8].

29 JD Mayne and H McGregor, *Mayne & McGregor on Damages* (Sweet & Maxwell, Limited, 12th ed, 1961) 196.

30 *Xl Petroleum (NSW) Pty Ltd v Caltex Oil (Australia) Pty Ltd* [1985] HCA 12 (28 February 1985) 471.

31 Ibid.

32 *Lamb v Cotogno* (1987) 164 CLR 1. They have been excluded for defamation and for negligence claims, but claims under the new tort for invasions of privacy will be more analogous to other intentional torts.

33 See, for example, *Defamation Act 2005* (NSW) s 35.

34 In *Giller v Procopets* (2008) 24 VR 1, the Victorian Court of Appeal denied the plaintiff an award of exemplary damages for breach of confidence, however the court did award damages for emotional distress. See also *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB) (2008) [172]–[197]. These decisions are in contrast to the NSW Supreme Court's decision in *Harris v Digital Pulse Pty Ltd* (2003) 56 NSWLR 298 which overturned an award of exemplary damages for breach of fiduciary duty.

35 This is in contrast to the UK approach: *Attorney General v Blake* [2000] UKHL 45 (27 July 2000).

11.34 However, unlike in defamation cases, there would be no presumption of harm in privacy cases, under the tort proposed in this Discussion Paper, and there may well be cases, such as *Kaye v Robertson*,[36] where the plaintiff may not be capable of suffering distress yet the circumstances of the invasion of privacy were outrageous and warrant exemplary damages to deter such conduct.

11.35 There is a legitimate concern that an award of exemplary damages provides a windfall to plaintiffs. Courts, however, are conscious of this concern and the High Court has ruled that awards of exemplary damages should be moderate.[37]

11.36 In addition to determining whether the exceptional circumstances of the case call for an award of exemplary damages, the court will also consider whether the other damages already awarded against the defendant are sufficient to fulfil the retributive, punitive or deterrent purposes of exemplary damages. In *NSW v Ibbett* the High Court when dismissing the appeal, quoted the earlier judgment of Spigelman CJ who stated that it is necessary,

> to determine both heads of compensatory damages before deciding whether or not the quantum is such that a further award is necessary to serve the objectives of punishment or deterrence or, if it be a separate purpose, condemnation.[38]

11.37 Views of stakeholders, previous inquiries in Australia and recent inquiries in the United Kingdom show a range of views on this issue.

11.38 Witzleb has suggested that 'exemplary damages should only be available as a last resort, i.e. where no other remedy would be a sufficient response to the wrong committed by the defendant'.[39]

11.39 The NSWLRC[40] recommended against allowing courts to award exemplary damages, noting the difficulty of reconciling exemplary damages with the purposes of the civil law. Analogous statutory actions such as defamation claims[41] and negligence claims for personal injury,[42] limit or exclude access to exemplary damages. The VLRC did not include exemplary damages in its recommendations.[43]

11.40 While a number of stakeholders supported courts being able to award exemplary damages,[44] often for similar reasons to those set out above, several stakeholders

---

36 *Kaye v Robertson* [1991] FSR 62.
37 *Xl Petroleum (NSW) Pty Ltd v Caltex Oil (Australia) Pty Ltd* [1985] HCA 12 (28 February 1985).
38 *New South Wales v Ibbett* (2006) 229 CLR 638, [34].
39 N Witzleb, *Submission 29*.
40 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill, cl 78. The ALRC previously adopted the same list of remedies, also excluding exemplary damages, but with no explanation on this last point; see ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [74.177].
41 See, for example, *Defamation Act 2005* (NSW) s 37.
42 See, for example, *Civil Liability Act 2002* (NSW) s 21.
43 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 29(a), [7.196]–[7.200].
44 Australian Privacy Foundation, *Submission 39*; Law Institute of Victoria, *Submission 22*; Women's Legal Centre (ACT & Region) Inc., *Submission 19*; I Turnbull, *Submission 5*; P Wragg, *Submission 4*; T Gardner, *Submission 3*.

opposed the availability of an award of exemplary damages.[45] The OAIC submitted that remedies for a privacy action should be directed at compensating a plaintiff, while exemplary damages are targeted at punishing a defendant.[46] There is also some concern that if exemplary damages were available, this may stifle important and legitimate activities like investigative journalism, and as such may restrict freedom of expression.

11.41 The UK's Leveson Inquiry recommended that courts be able to award exemplary or punitive damages for actions in breach of confidence, defamation and the tort of misuse of personal information.[47] Similarly, the Joint Committee of the House of Lords and House of Commons on Privacy and Injunctions in 2012 recommended that courts be empowered to award exemplary damages in privacy cases, arguing that compensatory damages were too low to act as an effective deterrent.[48] This recommendation led to the enactment of the *Crime and Courts Act 2013* (UK), which provides for the award of exemplary damages against a defendant who is a news organisation in misuse of information cases.[49]

11.42 Canadian privacy statutes also provide that courts may award punitive damages.[50]

Cap on damages

Proposal 11–6 The total of any damages other than damages for economic loss should be capped at the same amount as the cap on damages for non-economic loss in defamation.

11.43 The ALRC proposes a cap on damages for all damages other than for economic loss. This means that the total amount of general damages for non-economic loss and exemplary damages awarded would be capped at the same amount as the cap on damages for non-economic loss in defamation awards.[51] This proposal would ascribe equal weight to privacy and reputational interests. The proposal militates against the risk of plaintiffs cherry-picking between causes of action based on the availability of higher awards of damages.[52]

11.44 Restrictions on the scope of damages for non-economic loss for personal injury actions are stipulated at statute. For instance, in NSW, the initial cap was set at

45 SBS, *Submission 59*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*.
46 Office of the Australian Information Commissioner, *Submission 66*.
47 Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, House of Commons Paper 779 (2012) vol 4, [5.12].
48 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) 134.
49 *Crime and Courts Act 2013* (UK) s 34.
50 See, for example, *Privacy Act*, RSBC 1996, c 373.
51 See for example, *Defamation Act 2005* (NSW) s 35.
52 Nicholas Petrie, 'Reforming the Remedy: Getting the Right Remedial Structure to Protect Personal Privacy' (2012) 17 *Deakin Law Review* 139.

$350,000[53] and is now set at $551,500.[54] Damages for non-economic loss at defamation were initially capped at $250,000[55] and are now set at $355,000.[56]

11.45 In 2009, the NSWLRC proposed a cap on damages for non-economic loss for invasions of privacy of $150,000,[57] some $100,000 less than the defamation cap at the time.

11.46 David Rolph has argued that a cap on damages for a statutory cause of action should be higher than that stipulated at defamation law. He argued that a lower cap on damages for non-economic loss in privacy actions would be 'undesirable' as it fails to reflect the relative importance Australia should now prescribe to privacy.[58] Witzleb argued that existing caps on damages in other areas of Australian law were introduced to restrain what some perceived to be excessive compensation orders.[59] The ABC supported a cap on damages for non-economic loss, stating that the cap should not be higher than that at defamation law.[60]

11.47 Some stakeholders argued against a cap on damages.[61] The OAIC submitted that setting a cap 'may have the effect of focusing attention on that upper limit and implying that serious privacy invasions should result in a payout of that magnitude'.[62] However it will be at the court's discretion to make this assessment.

Account of profits

Proposal 11–7 The new Act should provide that a court may award the remedy of an account of profits.

11.48 The ALRC proposes that a court be empowered to award an account of profits.[63] This award would be an alternative to damages. The gains-based remedy of an account of profit will deter defendants who are commercially motivated to invade the privacy of another for profit, by removing any unjust gain made from a serious invasion of privacy.[64]

---

53 *Civil Liability Act 2002* (NSW) s 16. This includes a statutory indexation mechanism: s17.
54 Civil Liability (Non-Economic Loss) Amendment Order 2013.
55 See, for example, *Defamation Act 2005* (SA) ss 35, 35(4).
56 NSW Government Gazette No 65 of 31 May 2013. This figure is due to be increased on 1 July 2014.
57 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill, cl 77.
58 David Rolph, 'The Interaction of Remedies for Defamation and Privacy' [2012] *Precedent* 14.
59 N Witzleb, *Submission 29*.
60 ABC, *Submission 46*.
61 Office of the Australian Information Commissioner, *Submission 66*; Public Interest Advocacy Centre, *Submission 30*.
62 Office of the Australian Information Commissioner, *Submission 66*.
63 Several stakeholders were in favour of this proposal: Office of the Australian Information Commissioner, *Submission 66*; Public Interest Advocacy Centre, *Submission 30*; Insurance Council of Australia, *Submission 15*; I Turnbull, *Submission 5*.
64 N Witzleb, *Submission 29*. The ALRC proposed the availability of an account of profits in its previous Inquiry: ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(b).

11.49 In Australia, an account of profits is an equitable remedy that may be granted in cases where a defendant has profited from an equitable wrong. It is also available in some limited types of tort actions, such as passing off.[65] It is distinct from an award of damages in that it responds to the gain of the wrongdoer rather than the loss of the wronged party.[66] An account of profits will deter defendants who calculate that the gain to be made from publishing an individual's private information exceeds the cost of any compensatory damages they may incur if the matter goes to court.

11.50 An alternative way to achieve the same result would be to award exemplary damages to strip the defendant of any gain made from the unauthorised use of the plaintiff's information.[67]

11.51 This award is available as a remedy in breach of confidence actions.[68] In *Douglas v Hello! Ltd (No 3),* the UK Court of Appeal made clear that it would have had 'no hesitation to award an account of profits'[69] if 'Hello!' magazine had made a profit from the publication of surreptitiously obtained photographs of the wedding of Michael Douglas and Catherina Zeta-Jones.

11.52 It may however be difficult to prove that the defendant has made any profit or gain from the invasion of privacy. Media publication of private information may often be unsuited to the award of an account of profit because the story may be only one part of the media program or edition and cannot be attributed with a distinct amount of profit.

11.53 An account of profits was recommended as a remedy for a serious invasion of privacy in ALRC Report 108.[70] The NSWLRC also recommended an account of profits, at least in exceptional cases.[71] Both commissions noted the concerns of some stakeholders that it would in many cases be difficult to determine the profits arising from a serious invasion of privacy, but neither commission considered that this should more generally preclude an account of profits being available.

Damages based on notional licence fee

Proposal 11–8 The new Act should provide that courts may award damages assessed on the basis of a notional licence fee in respect of the defendant's conduct, in an action for serious invasion of privacy.

65 RP Meagher, JD Heydon and MJ Leeming, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 4th ed, 2002) [25–002].
66 *Warman International Ltd v Dwyer* (1995) 182 CLR 544.
67 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 497.
68 *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB) (2008); *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109.
69 *Douglas v Hello! Ltd* [2005] EWCA Civ 595 (18 May 2005) [200].
70 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5.
71 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [7.23]–[7.24].

11.54 Damages assessed on the basis of a notional licence fee would require the defendant to pay to the plaintiff any sum that the plaintiff would have received if the defendant had asked prior permission to carry out the activity that invaded the plaintiff's privacy. An assessment of damages calculated on the basis of a notional licence fee is a remedy which seeks to target the value to the defendant of deliberately invading the plaintiff's privacy.

11.55 The possibility of an assessment of damages on the basis of a notional licence fee was discussed by Hodgson J in *LJP Investments Pty Ltd v Howard Chia Pty Ltd*, a case involving trespass to land by the erection of scaffolding into the plaintiff's airspace:

> [I]n my view, if what is used has peculiar value for a defendant, then damages under this head should reflect that value, rather than the general market value. For example, if a plaintiff is the last tenant in a development site, and is forcibly ejected and the building immediately demolished; and if the defendant acted on incorrect legal advice that he was entitled to do this, so that he may be able to escape exemplary damages; then I think the plaintiff's damages should not be limited to the general market value of the plaintiff's tenancy, but should reflect he price which the plaintiff and defendant would reasonably have negotiated, having regard to the plaintiff's position and the defendant's wish to develop the site.[72]

11.56 Damages assessed on the basis of notional licence fees have been considered by courts in the UK. In *Irvine v Talksport*[73] 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. In *Douglas v Hello!(No 3)* the UK Court of Appeal recognised the availability of a hypothetical-fee award in situations where a plaintiff had permitted to the invasive act in question but had not been compensated for the use of their image.[74]

11.57 The assessment of damages based on the calculation of a notional licence fee is consistent with the fault requirement of the statutory cause of action proposed in this Discussion Paper—confined to intentional acts—as a notional licence fee would target defendants who had deliberately set out to enrich themselves or save expense by invading an individual's privacy.

11.58 Sirko Harder examined the argument that the exclusive right to authorise use of one's image is a commercial publicity right.[75] Harder argued that a publicity right is akin to a property right which is transferable, as distinguished from an individual's privacy interests which are not assignable in a proprietorial sense. However, there are cases where private information is provided in return for a monetary value. For instance, individuals who enter into contractual arrangements to disclose their private information such as 'tell-all interviews' on television—often in exchange for monetary

---

72 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1990) 24 NSWLR 499, 507.

73 *Irvine v Talksport Ltd* (2003) 2 ER 881.

74 Sirko Harder, 'Gain-Based Relief for Invasion of Privacy' (2011) 1 *DICTUM-Victoria Law School Journal* 63, 68.

75 Ibid 74.

compensation—attach some monetary value to their private information. Moreover, Harder argued that gain-based remedies are appropriate to remedy invasions of privacy given that

> the right to privacy constitutes a right to exclude others from one's private sphere and thus an exclusive entitlement against the whole world. … Gain-based relief is the natural consequence of the unauthorised use of an exclusive entitlement.[76]

11.59 Also in favour of gain-based remedies in privacy actions, Witzleb argued that 'gain-based relief as a less intrusive, and more carefully targeted, remedy should be preferred as the primary defendant-focused remedy in privacy cases'.[77]

Contributory negligence should not be considered in assessing damages

11.60 The ALRC does not propose that contributory negligence be included as a factor to be considered by a court to reduce an award of damages. Under state apportionment legislation, a court may reduce an award of damages in certain claims to the extent that the plaintiff was at fault,[78] but only where the defence of contributory negligence would have been a complete defence at common law. Contributory negligence is not a defence at common law to intentional torts and the apportionment legislation therefore does not apply to such claims.[79]

11.61 Including contributory negligence as a factor in the assessment of damages would be inconsistent with the fault element of the proposed statutory cause of action which limits liability to intentional or reckless conduct.

Injunctions

Proposal 11–9 The new Act should provide that courts may award an injunction, in an action for serious invasion of privacy.

11.62 The availability of an order of injunctive relief to prevent or restrain the publication of private information is an important protection proposed by the ALRC. In privacy actions, plaintiffs are likely to seek interlocutory or interim injunctions to prevent the commission or continuance of a serious invasion of privacy. For example, a plaintiff may seek to prevent the publication of their personal information by a media outlet. Given the fragile nature of privacy, preventing the irreparable harm of publication or disclosure of private information is critical.

---

76 Ibid 79.

77 Normann Witzleb, 'Justifying Gain-Based Remedies for Invasions of Privacy' (2009) 29 *Oxford Journal of Legal Studies* 325, 355.

78 See, for example, *Law Reform (Miscellaneous Provisions) Act 1965* (NSW) s 9.

79 *Horkin v North Melbourne Football Club* (1983) 1 VR 153.

11.63 The availability of an interim or interlocutory injunction to restrain publication may, in some cases, reduce or eliminate the need for further litigation or the need for a court to grant other remedies.

11.64 Previous law reform inquiries recommended that courts be able to order injunctive relief.[80] Principles relating to injunctive relief in privacy cases are discussed further in Chapter 12.

Delivery up, destruction or removal of material

Proposal 11–10 The new Act should provide that courts may order the delivery up and destruction or removal of material, in an action for serious invasion of privacy.

11.65 Orders for the delivery up, destruction or removal of material will be an appropriate remedy for serious invasions of privacy where a defendant has obtained private information about a plaintiff and has exhibited an intention to disclose that information to a third party. This may arise in a situation where two people in an intimate relationship share images or text of a highly personal nature and, at the end of the intimate relationship, one party intends to publish or disclose those images to a third party. In such a case, courts may order that the material be delivered to a court and destroyed. Several stakeholders supported this proposal.[81]

11.66 The ALRC intends this power to extend to orders for the take-down of online content which amounts to a serious invasion of privacy. A court may order that an online provider or an individual who controls their own website (such as a blogger) must remove or take-down specific content. An analogous provision exists at s 133 of the *Copyright Act 1968* (Cth), which empowers a court to order the delivery up and destruction of material which violates copyright law.

11.67 Australian courts have existing powers to issue similar orders. For instance, Anton Pillar orders are a form of mandatory injunction, issued by a court to prevent the destruction of evidence.[82] Anton Pillar orders are issued when a court considers that a defendant is likely to destroy documents or property necessary for proceedings.[83]

11.68 The NSWLRC and ALRC[84] previously recommended that courts be empowered to make an order for the delivery up and destruction of material. The NSWLRC recommended that courts be empowered to order a defendant to deliver to a plaintiff

80 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(c).
81 Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; T Gardner, *Submission 3*.
82 Bernard Cairns, *Australian Civil Procedure* (Thomson Reuters (Professional) Australia, 8th ed, 2009) [13.80].
83 *Long v Specifor Publications Pty Ltd* (1988) 44 NSWLR 545, [547] (Powell JA).
84 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(f).

any 'articles, documents or material (and any copies), that were made or disclosed as a result of the invasion'.[85]

11.69 The OAIC and PIAC suggested that, in an action under the new tort, courts be able to make an order requiring a defendant to rectify its business or IT practices to redress systemic problems with the way it stores private information.[86] The ALRC has not proposed such an order as such systemic problems would generally be the result of negligent acts or omissions and be more appropriately dealt with by the regulator. The cause of action proposed in this Discussion Paper is confined to intentional or reckless invasions of privacy.

Correction orders

Proposal 11–11 The new Act should provide that courts may make a correction order, in an action for serious invasion of privacy.

11.70 The ALRC proposes that courts be given the power to order defendants to publish, in appropriate terms, a correction.[87] Such an order can set the record straight, and may be necessary where, for example, the defendant disclosed *untrue* private information about the plaintiff.

11.71 The disclosure of private information may amount to a serious invasion of privacy despite the information being untrue.[88] Private information can include information which is true or false so long as it has a quality of privacy, that is, the subject matter of the information is sufficiently private or personal in nature so that its disclosure would cause emotional distress to a relevant individual. In the Canadian case of *Ash v McKennit*, Longmore J noted:

> The question in a case of misuse of private information is whether the information is private, not whether it is true or false. The truth or falsity of the information is an irrelevant inquiry in deciding whether the information is entitled to be protected and judges should be wary of becoming side-tracked into that irrelevant inquiry. [89]

11.72 Correction orders may reduce the need for a plaintiff's interests to be vindicated through an award of damages.[90] Some plaintiffs may be primarily concerned with correcting the public record, in which case the advantage of correction orders is they

---

85 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWRC Draft Bill, cl 76(1)(d).

86 Office of the Australian Information Commissioner, *Submission 66*. The OAIC suggested this power would be similar in nature to the OAIC's power to instigate an own-motion investigation under the *Privacy Act 1988* (Cth).

87 Australian law provides discretion to a court to issue coercive correction orders, for example, *Australian Consumer Law* (Cth) 246(2)(d). In defamation law, a court does not have the discretion to issue a correction order, however whether a defendant has made an apology or a correction order can be taken into account when assessing the 'reasonableness' of any offer of amends, for example in *Defamation Act 2005* (NSW) s 14.

88 See Ch 5.

89 *McKennitt v Ash* [2008] QB 73, 86.

90 Carroll and Witzleb, above n 14, 236.

appear in the original publication and therefore target the same audience. Witzleb and Carroll have made the point that in actions to restore personality interests, monetary remedies may be ill-suited.[91] Instead, coercive methods such as public corrections may be more appropriate to reverse or reduce the effect of an invasion of privacy which has demeaned and distressed the plaintiff in a public forum.

11.73 The Australian Subscription Television and Radio Association (ASTRA) opposed any remedies which would compel corrections, arguing that media organisations are already subject to similar provisions in ASTRA Codes which are registered with the ACMA.[92] However there may be instances where a plaintiff is awarded a range of remedies as part of the cause of action including damages and an order for apology. In such cases, the availability of those remedies in a single cause of action will provide simplicity for all parties to a proceeding. A plaintiff would not need to pursue a defendant through both a regulatory scheme and through the courts in relation to the same serious invasion of privacy. Furthermore, if a defendant has already made a statement involving a correction, this will mitigate an award of damages.[93]

Apology orders

Proposal 11–12 The new Act should provide that courts may make an order requiring the defendant to apologise to the plaintiff, in an action for serious invasion of privacy.

11.74 The availability of an order requiring a defendant to apologise would, in some circumstances, vindicate the hurt and distress caused to a plaintiff by a serious invasion of privacy.[94] Given the aim of the tort is to redress harm done to a personal, dignitary interest, an apology may assist in rectifying a plaintiff's feelings of embarrassment and distress. Witzleb and Carroll argued that orders for apology help to 'redress the injury by restoring the plaintiff's dignity and personality'.[95] Similarly, Prue Vines has argued:

> Apologies are also a tool of communication and of emotion. Apologies may redress humiliation for the victim, shame the offender and help to heal the emotional wounds associated with a wrong.[96]

11.75 The purpose of a plaintiff seeking an order for apology will depend on the circumstances of each case, but may involve the need for acknowledgement of their suffering.[97] The publicity garnered by a public statement of apology may help to

91 Ibid, 233.
92 Australian Subscription Television and Radio Association, *Submission 47*.
93 See Proposal 6-3.
94 Insurance Council of Australia, *Submission 15*; I Pieper, *Submission 6*; I Turnbull, *Submission 5*.
95 Carroll and Witzleb, above n 14, 237.
96 Prue Vines, 'The Power of Apology: Mercy, Forgiveness or Corrective Justice in the Civil Liability Arena?' (2007) 1 *Public Space* 1, 15.
97 Robyn Carroll, 'Apologies as a Legal Remedy' (2013) 35 *Sydney Law Review* 317, 337.

'restore the esteem and social standing which has been lost as a consequence of the contravention'.[98]

11.76 The ALRC previously recommended that courts be empowered to order a defendant to apologise.[99] The NSWLRC recommended that the defendant's conduct—including whether they had apologised or made an offer of amends prior to proceedings—should be taken into account when determining actionability.[100] The VLRC did not recommend such an order be available to a court, however the VLRC's final report stated:

> Sometimes it may be appropriate to direct a person to publish an apology in response to the wrongful publication of private information or to apologise privately, for an intrusion into seclusion.[101]

11.77 Australian law recognises the significance of apologies where there has been damage to personality or reputation in a range of actions at statute, equity and at the common law.[102] For example, a court may order an apology under Commonwealth and state anti-discrimination legislation.[103] This area of law is analogous to privacy actions in that anti-discrimination law aims to remedy damage to feelings. Similarly, in defamation law, a court may take a publisher's apology for defamatory matter into account when assessing damages.[104]

11.78 Public apologies may also serve to educate the public about privacy and deter future serious invasions of privacy.[105] A plaintiff may value the public vindication an apology brings.

11.79 In *Burns v Radio 2UE Sydney Pty Ltd (No 2)*, the NSW Anti-Discrimination Tribunal defined a court-ordered apology as an acknowledgement of 'wrongdoing' that is distinguished from a personal apology which is 'sincere and which is incapable of being achieved by a court order'.[106]

Declarations

Proposal 11–13 The new Act should provide that courts may make a declaration, in an action for serious invasion of privacy.

---

98 *Eatock v Bolt (No 2)* (2011) 284 ALR 114, [15].

99 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–5(d).

100 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWRC Draft Bill, cl 74(3)(a)(vi).

101 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.207].

102 Carroll, above n 97, 213.

103 See, for example, the Anti-Discrimination Tribunal of NSW is empowered to issue an order requiring a respondent to publish or issue an apology or retraction: *Anti-Discrimination Act 1977* (NSW) s 108. Apologies made by respondents in personal injury matters are not treated as evidence of admission of fault: *Civil Liability Act 2002* (NSW) s 69.

104 See, for example, *Defamation Act 2005* (NSW) s 38.

105 Carroll, above n 97, 339.

106 *Burns v Radio 2UE Sydney Pty Ltd (No 2)* [2005] NSWADTAP 69 (6 December 2005).

11.80 The availability of declaratory relief will provide applicants with a sense of certainty and may avoid lengthy and costly court proceedings.[107] Several stakeholders submitted that declaratory relief should be availabile.[108]

11.81 A declaration in an action for serious invasion of privacy will take the form of a non-coercive order by a court that states the nature of the interests, rights or duties of the applicant to an action.[109] Their availability will provide both parties to a proceeding with clarity as to their obligations and rights in order to avoid future litigation. A declaration may establish that a plaintiff has enforceable rights which may be upheld at a later date if the wrong continues. Similarly, a declaration may declare that future conduct by a defendant (or possible defendant) will not be a 'breach of contract or law'.[110]

11.82 Declarations are available in a variety of areas of Australian law.[111] Section 21 of the *Federal Court Act 1976* (Cth) provides that the court may make a declaration on the legality of another party's conduct.[112] The ACCC has sought declarations under this provision in numerous cases in order to determine whether a party has violated Australian consumer law.[113]

11.83 The ALRC, NSWLRC and VLRC previously proposed that courts be able to make declarations.[114]

11.84 ASTRA opposed the availability of declarations, arguing that the ACMA's existing powers provide it with the power to require a licensee to acknowledge a finding of the ACMA on the licensee's website. Section 205W of the *Broadcasting Services Act 1992* (Cth) provide the ACMA with the power to accept undertakings from broadcasters on a range of matters. However, the availability of declaratory relief will have a significant normative impact on the future conduct of a defendant, given the risk of monetary remedies if legal rights which have been the subject of a judicial pronouncement are contravened.

11.85 The operation of a declaration will not affect the availability of other remedies, if a court exercises their discretion to award other appropriate remedies.

---

107 Meagher, Heydon and Leeming, above n 65, [19–180].

108 N Witzleb, *Submission 29*; Public Interest Advocacy Centre, *Submission 30*.

109 Cairns, above n 82, [1.20].

110 *Bass v Permanent Trustee Co Ltd* (1999) CLR 198 334, [356] (Bass v Permanent Trustee Co Ltd (1999) 198 CLR 334, [356] (Gleeson CJ, Gaudron, McHugh, Gummow, Hayne and Callinan JJ).

111 Meagher, Heydon and Leeming, above n 65, [19–075].

112 *Federal Court of Australia Act 1976* (Cth) s 21. 'The Court may, in civil proceedings in relation to a matter in which it has original jurisdiction, make binding declarations of right, whether or not any consequential relief is or could be claimed': s 21(1).

113 *Australian Competition & Consumer Commission v Black on White Pty Ltd* [2001] [2001] FCA 187 (6 March 2001).

114 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(g); NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWRC Draft Bill, cl 76(1)(c); Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 29(c).

Costs

Question 11–1 What, if any, provisions should the ALRC propose regarding a court's power to make costs orders?

11.86 At this stage in the Inquiry, the ALRC has not made a proposal on a court's power to make costs orders in a cause of action for serious invasion of privacy. The ALRC welcomes stakeholder feedback on this issue. The ALRC is particularly interested in the issue of costs in the context of ensuring access to justice.[115]

11.87 The VLRC recommended that costs be dealt with in accordance with s 130 of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic).[116] That section provides that each party should bear their own costs in a proceeding, unless the Tribunal orders one party to pay all or a part of the costs of the other party, if that would be fair to do so. This recommendation is consistent with the VLRC's recommendation that their proposed privacy actions be heard in the VCAT. Any proposal on costs will depend on the forum in which a statutory cause of action is heard.

11.88 PIAC's submission raised the concern that many plaintiffs will be deterred from starting proceedings due to the risk of an adverse costs order.[117] PIAC suggested that if the cause of action were to be vested in a federal court, the ALRC should propose that courts be empowered to make orders protecting litigants from adverse costs orders.

11.89 Special provisions about costs orders may be made in the legislation enacting the statutory cause of action, or it may be preferable to rely on any discretion given to the court hearing the matter under its own enabling legislation.

115 The OAIC's submission raised costs as an issue which influences the accessibility of civil proceedings: Office of the Australian Information Commissioner, *Submission 66*.

116 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 30.

117 Public Interest Advocacy Centre, *Submission 30*.

Part 3

12. Breach of confidence actions for misuse of private information

Contents

Summary

12.1 This chapter makes two proposals dealing with existing protections of privacy at common law and with a view to the likely development of the common law if a statutory cause of action is not enacted.[1]

12.2 In addition to and separate from the detailed legal design of a statutory cause of action for serious invasion of privacy, the Terms of Reference require the ALRC to make recommendations as to other legal remedies to redress serious invasions of privacy and as to innovative ways in which the law may reduce serious invasions of privacy.

12.3 The Terms of Reference also direct the ALRC to make recommendations as to the necessity of balancing the value of privacy with other fundamental values including freedom of expression and open justice.

12.4 The first proposal is intended to redress uncertainty in the community as to whether Australian law provides a remedy for emotional distress suffered as a result of a breach of privacy which takes the form of the disclosure or misuse of private

1 In this chapter, the ALRC does not consider the possible development at common law of a new or separate tort for harassment or intrusion into seclusion, because it considers that, in the absence of a statutory cause of action for serious invasion of privacy, a *statutory* action for protection against harassment is the more appropriate way for the law to be developed: see Ch 14. If, however, the common law were to develop a tort of harassment or a tort of invasion of privacy by intrusion into seclusion, it would be necessary for the courts expressly to identify its elements, including whether: it was actionable per se, by analogy with trespass to the person; required damage in the usual sense of psychiatric or physical illness; or required damage but including emotional distress.

(possibly confidential) information.[2] The first proposal is that courts be empowered to award compensation for emotional distress in such cases.

12.5 The ALRC also proposes that countervailing public interests, including freedom of expression, be considered by a court in an application to prevent publication of private information. This may be particularly important if the tort proposed in this Discussion Paper is not enacted, and greater protections against disclosure of private information instead develop at common law. It is unclear what principles should govern the exercise of the court's discretion in any action to protect merely private (not confidential) information. Australian case law provides only a very limited role for public interest considerations as a justification for restraining the breach of an obligation of confidence. By contrast, defamation law incorporates well-established principles which protect freedom of speech. The ALRC considers that there should be protections for freedom of speech in applications to prevent the disclosure of private, but not confidential, information.

The likely future development of the action for breach of confidence

12.6 In *ABC v Lenah Game Meats* Gleeson CJ appeared to foreshadow that the equitable action for breach of confidence may be the most suitable legal action for protecting people's *private* information from disclosure, stating:

> [E]quity may impose obligations of confidentiality even though there is no imparting of information in circumstances of trust and confidence. And the principle of good faith upon which equity acts to protect information imparted in confidence may also be invoked to 'restrain the publication of confidential information improperly or surreptitiously obtained'. The nature of the information must be such that it is capable of being regarded as confidential. A photographic image, illegally or improperly or surreptitiously obtained, where what is depicted is private, may constitute confidential information …
>
> If the activities filmed were private, then the law of breach of confidence is adequate to cover the case … There would be an obligation of confidence upon the persons who obtained [images and sounds of private activities], and upon those into whose possession they came, if they knew, or ought to have known, the manner in which they were obtained …
>
> The law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy.
>
> 55. For reasons already given, I regard the law of breach of confidence as providing a remedy, in a case such as the present, if the nature of the information obtained by the trespasser is such as to permit the information to be regarded as confidential.[3]

---

2 This proposal would not, therefore, apply to cases involving commercial information or the like. In this chapter, the ALRC intends 'private' information to mean information as to which a person in the position of the plaintiff has a reasonable expectation of privacy in all of the circumstances.

3 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [34], [39], [40], [55].

12.7 Gummow and Hayne JJ, with whom Gaudron J agreed, considered a broader range of privacy invasions and left open the direction that the future development of the law protecting privacy may take:

> In the present appeal Lenah encountered … difficulty in formulating with acceptable specificity the ingredients of any general wrong of unjustified invasion of privacy. Rather than a search to identify the ingredients of a generally expressed wrong, the better course, as Deane J recognised [in *Moorgate Tobacco Ltd v Philip Morris Pty Ltd (No 2)*[1984] HCA 73; (1984) 156 CLR 414, 444-445], is to look to the development and adaptation of recognised forms of action to meet new situations and circumstances …
>
> Lenah's reliance upon an emergent tort of invasion of privacy is misplaced. Whatever development may take place in that field will be to the benefit of natural, not artificial, persons. It may be that development is best achieved by looking across the range of already established legal and equitable wrongs. On the other hand, in some respects these may be seen as representing species of a genus, being a principle protecting the interests of the individual in leading, to some reasonable extent, a secluded and private life, in the words of the *Restatement*, 'free from the prying eyes, ears and publications of others'. Nothing said in these reasons should be understood as foreclosing any such debate or as indicating any particular outcome.[4]

12.8 Despite this influential and open invitation to the courts to develop further protection, there has been only isolated development at common law of further privacy protection in Australia, as discussed in Chapter 3 above, making it difficult to predict the precise direction of future developments.[5] Both of the proposals in this chapter assume that, in the absence of a statutory cause of action, the development of the equitable action for breach of confidence is the most likely way in which the common law may, in time, develop greater protection of privacy in relation to disclosure of private information.

Damages for emotional distress in action for breach of confidence

Proposal 12–1 If a statutory cause of action for serious invasion of privacy is not enacted, appropriate federal, state, and territory legislation should be amended to provide that, in an action for breach of confidence that concerns a serious invasion of privacy by the misuse, publication or disclosure of private information, the court may award compensation for the claimant's emotional distress.

---

4 Ibid [110], [132].

5 *Hosking v Runting* (2005) 1 NZLR 1, [56]–[59] (Gault P and Blanchard J): 'The recent High Court of Australia decision in *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* does little to clarify the future direction of Australian jurisprudence'. The Australian cases dealing with issues relating to invasions of privacy are set out in Ch 3.

12.9 There are several arguments in favour of the ALRC's proposal. First, if legislation clarified or confirmed that compensation could be awarded for emotional distress, the *existing* action for breach of confidence would more readily be seen as a useful response to serious invasions of privacy, and be more attractive to potential claimants.[6] This is particularly important in the event that the statutory cause of action is not enacted. Secondly, the effectiveness and availability of the remedy may deter invasions of privacy involving disclosures of private information. Thirdly, this proposal would be an effective way of addressing a significant gap in existing legal protection of privacy while being more limited and directed than the introduction of a new statutory cause of action. Fourthly, this provision would also indicate that Australian legislatures intended that the action for breach of confidence could be relied on to remedy these kinds of invasions of privacy.

12.10 In traditional claims for breach of confidence in Australia, claimants have generally sought one of three remedies: an injunction to restrain an anticipated or continuing breach of confidence; compensation for economic loss due to a breach; or an account of the anticipated profits derived from a breach. This has been so, whether the relevant confidence concerned commercial, governmental or personal information.

12.11 However, where a breach of confidence in relation to *personal* confidential or private information has already occurred and an injunction is futile, the consequence that a claimant is most likely to suffer is emotional distress, rather than harm in the nature of economic loss.[7] Professor Michael Tilbury has noted that 'the very object of the action [for invasion of privacy] will be to protect plaintiffs against [mental or emotional distress], at least in part.'[8]

12.12 The Law Institute of Victoria submitted that 'harm caused by breaches of privacy is more likely to be harm such as embarrassment, humiliation, shame and guilt. Given the centrality of privacy to identity, these harms should not be seen as insignificant, even though they are not physical or financial'.[9]

12.13 While the limited circumstances for the recovery of compensation for 'mere' emotional distress, even intentionally caused, has been a perennial issue for the law of

---

6 Normann Witzleb, 'Giller v Procopets: Australia's Privacy Protection Shows Signs of Improvement' (2009) 17 *Torts Law Journal* 121, 123–124: 'Considering that breach of confidence will, until more specific protection is in place, continue to act as Australia's quasi-privacy tort, courts need to afford adequate protection against emotional distress.'

7 A claimant may suffer some other harm that the law accepts as actual damage, such as personal or psychiatric injury.

8 Michael Tilbury, 'Coherence, Non-Pecuniary Loss and the Construction of Privacy' in Jeffrey Berryman and Rick Bigwood (eds), *The Law of Remedies: New Directions in the Common Law* (Irwin Law, 2010) 127, 140. Note also: *Privacy Act 1988* (Cth) s 52(1) provides that the Information Commissioner investigating a complaint concerning a breach of that Act may make a determination that the complainant is entitled to compensation for loss, which is defined to include injury to the complainant's feelings or humiliation suffered by the complainant.

9 Law Institute of Victoria, *Submission 22*.

torts,[10] the issue of recovery in equity had not been raised in Australia until the case of *Giller v Procopets,*[11] decided by the Supreme Court of Victoria Court of Appeal in 2008. In that case, Neave JA noted: 'The Australian position appears to be at large on this issue. I am not aware of any appellate court decision which has considered it.'[12] Ashley JA stated: 'No Australian authority was cited at trial or on appeal to support the proposition that, in the context now under discussion, equitable compensation or equitable damages … can be awarded for mental distress alone.'[13]

12.14 In *Giller v Procopets* the court held that the claimant could recover damages for emotional distress in her equitable claim for breach of confidence. The claim was clearly one for breach of confidence, as the material that had been disclosed by the defendant, a videotape of intimate activities, had been created by the claimant and defendant while in a de facto relationship. The court unanimously agreed that the claimant could recover compensation for her consequent emotional distress as equitable compensation. Neave JA, with whom Maxwell JA agreed, also upheld the award as damages under the Victorian equivalent of *Lord Cairns' Act*,[14] s 38 of the *Supreme Court Act 1986* (Vic).[15] An application by Procopets to the High Court of Australia for leave to appeal was rejected.[16]

12.15 There are several reasons why it would be desirable for legislation to clarify the courts' powers to award compensation for emotional distress, notwithstanding the judgment in *Giller v Procopets.*

12.16 First, at the time of this Discussion Paper, *Giller v Procopets* remains the sole appellate authority for the recovery of compensation of emotional distress in a breach

---

10 Unlike the position in the United States, Australian courts, like those in the United Kingdom and elsewhere, do not recognise a cause of action for wilful infliction of emotional distress. The tort action for wilful infliction of nervous shock, known as the action under *Wilkinson v Downton* (1897) 2 QB 57 is an 'action on the case', and like an action in negligence, requires proof of actual damage, such as a recognised psychiatric illness: *Giller v Procopets* (2008) 24 VR 1 (Neave JA & Ashley JA, Maxwell P dissenting); *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417; *Wainwright v Home Office* [2004] 2 AC 406. See further, Barbara McDonald, 'Tort's Role in Protecting Privacy: Current and Future Directions' in James Edelman, James Goudkamp and Degeling (eds), *Torts in Commercial Law* (Thomson Reuters, 2011).

11 *Giller v Procopets* (2008) 24 VR 1.

12 Ibid [419].

13 Ibid [133].

14 A statute following *Lord Cairns' Act* (21 & 22 Vict c 27) *1858* generally provides, in brief, that where a court has power to grant an injunction or to order specific performance, the court may award damages to the party injured either in addition to or in substitution for the injunction or specific performance. An example of the common form is s 68 of the *Supreme Court Act 1970* (NSW). Section 38 of the *Supreme Court Act 1986* (Vic) has different wording: 'If the Court has jurisdiction to entertain an application for an injunction or specific performance, it may award damages in addition to, or in substitution for, an injunction or specific performance'.

15 Ashley JA in *Giller v Procopets* (2008) 24 VR 1 at [141] did not agree that s 38 empowered the award: 'I should next say that, upon the question of the availability of damages for mental distress, the common law would provide no assistance to the appellant even if s 38 was treated as making common law remedies available in a case within the exclusive jurisdiction. With few exceptions, the common law has turned its face against awards of damages for distress.' Later at [148]: 'But that does not mean that equity must do so'. He supported the award of compensation under the exercise of equity's inherent jurisdiction.

16 *Procopets v Giller (M32/2009)* [2009] HCASL 187.

of confidence action, over five years after it was decided. The position reached in that case has not been further tested or applied in Australia. Prior to that decision, a county court judge in Victoria, in the 2007 case of *Doe v Australian Broadcasting Corporation,* awarded equitable compensation of $25,000 for breach of confidence, for 'hurt, distress, embarrassment, humiliation, shame and guilt', as part of a larger award for other wrongs.[17] The case was settled before appeal.

12.17 Secondly, s 38 of the *Supreme Court Act 1986* (Vic), relied upon to justify the award of compensation in *Giller v Procopets*, differs from the form of *Lord Cairns' Acts* in other jurisdictions[18] where there is still controversy as to whether *Lord Cairns' Act* applies in aid of purely equitable rights such as breach of confidence.[19]

12.18 Thirdly, even if *Lord Cairns' Act* or s 38 of the *Supreme Court Act 1986* (Vic) does apply, this does not explain the basis on which equity can award compensation, in the form of common law compensatory damages and aggravated damages, for emotional distress arising from the breach of an equitable wrong. Regardless of the wording of the statute, it is problematic to have an equitable grant of compensation or 'damages' by analogy with tort law: as Ashley JA points out, 'with few exceptions, the common law has turned its face against awards of damages for distress'[20] and, as the majority held, tort law would not have provided a remedy in the circumstances. This point is *not* an argument that the judgment undesirably fuses law and equity.[21] Rather it is an argument based on the need for legal coherence.

12.19 Fourthly, if the award for emotional distress in *Giller v Procopets* is better treated as an award of equitable compensation, there remains an unsettling lack of precedent for the decision. Further it is arguably inconsistent with another decision in which a state appellate court rejected a claim in an equitable action for punitive damages, previously only given at common law.[22] While the courts of the United Kingdom, starting with *Campbell v MGN Ltd* in 2004, have routinely awarded

---

17 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, [186].

18 *Supreme Court Act 1970* (NSW) s 68; *Supreme Court Act 1935* (SA) s 30; *Supreme Court Act 1935* (WA) s 25; *Supreme Court Civil Procedure Act 1932* (Tas) s 11; *Judicature Act 1876* (Qld) s 4; RP Meagher, JD Heydon and MJ Leeming, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 4th ed, 2002), [23–030]. See above n 14.

19 Tanya Aplin et al, *Gurry on Breach of Confidence* (Oxford University Press, 2nd ed, 2012) [19.11] states that some courts 'have taken the view that *Lord Cairns' Act* could, and should, apply to confidence claims', but that 'leading commentators continue to argue that *Lord Cairns' Act* had no effect on causes of action which were purely equitable (such as breach of confidence), rather in such cases equitable compensation should be awarded.' See also Ibid [19.15] and *Cadbury Schweppes v FBI Foods* [2000] FSR 491.

20 *Giller v Procopets* (2008) 24 VR 1, [141].

21 Aplin et al, above n 19, [17.13] notes the 'acceptance by the courts in most common law jurisdictions that (in relation to remedies at least) the rules of equity and law can be moulded to do practical justice means that the availability of remedies for breach of confidence are not, and should not be, confined by the nature of the jurisdiction upon which the claim is based. Rather the approach the court adopts should be flexible with the full panoply of remedies being available in appropriate cases. Nevertheless, this approach is not at present acknowledged by the Australian courts, and there is some indication that fusion has not been fully embraced elsewhere.'

22 *Harris v Digital Pulse Pty Ltd* (2003) 56 NSWLR 298.

damages for emotional distress in the so-called 'extended' action of breach of confidence which protects against disclosures of private information, they are clearly underpinned by the requirements of the *Human Rights Act 1998* (UK), which provides a very different remedial framework from that in the Australian legal system.

12.20 However, equity is traditionally seen as having a great deal of remedial flexibility and, provided the award is seen as consistent with broad equitable principles and doctrines, a lack of precedent may not be a significant problem.[23] Gummow J has contrasted the approach of equity to the common law:

> The common law technique … looks to precedent and operates analogically as a means of accommodating certainty and flexibility in the law. *Equity, by contrast, involves the application of doctrines themselves sufficiently comprehensive to meet novel cases.* The question of a plaintiff 'what is your equity?'[as posed by Gleeson CJ in *ABC v Lenah Game Meats Pty Ltd*[24]] thus has no common law counterpart.[25]

12.21 Further, there is much strength in the simple point made by Neave JA, that '[a]n inability to order equitable compensation to a claimant who has suffered distress would mean that a claimant whose confidence was breached before an injunction could be obtained would have no effective remedy.'[26] On these grounds, it is strongly arguable that compensation for emotional distress *should* be part of the armoury of remedies available to a court of equity when determining a claim for breach of confidence through the disclosure of private information.

12.22 It may well be that courts will arm themselves with this power by following the lead of *Giller v Procopets* in the future. However, the position would be rendered more certain, and there would be less room for argument and expensive litigation along the way, if legislation were the source of that power. As Gurry has commented, '[a]ny discussion of the application of the remedy of damages in breach of confidence cases is fraught with difficulty at the outset'.[27] It is therefore highly desirable that there be *some* legislative clarification.

Injunctions, privacy and the public interest

Proposal 12–2 Relevant court acts should be amended to provide that, when considering whether to grant injunctive relief before trial to restrain publication of private (rather than confidential) information, a court must have particular regard to freedom of expression and any other countervailing public interest in the publication of the material.

---

23 *Harris v Digital Pulse Pty Ltd* (2003) 56 NSWLR 298, 304 (Spigelman CJ), quoted in *Giller v Procopets* (2008) 24 VR 1, [436] (Neave JA).

24 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 216.

25 *Roads and Traffic Authority of New South Wales v Dederer* (2007) 324 CLR 330, [57] (emphasis added).

26 *Giller v Procopets* (2008) 24 VR 1, [424]. Cf [168]–[169] (Gillard J).Ibid [424], ibid [168]–[169].

27 Aplin et al, above n 19, [19.02].

12.23 An interlocutory injunction is the most significant remedy to prevent a threatened invasion of privacy, such as the broadcast or publication of private information. However, of all remedies, an interlocutory injunction restraining publication is also the most significant restriction on freedom of speech and the freedom of the media to report on matters of public interest and concern.

12.24 There is a strong and justifiable concern that undue restrictions upon freedom of speech and the freedom of the press might arise from unmeritorious claims to prevent the disclosure of allegedly 'private' information in which there is a legitimate public interest.

12.25 The ALRC proposes that courts should be directed by appropriate legislation to consider countervailing interests in freedom of expression and other matters of public interest when considering the award of an interlocutory injunction to restrain the publication of private information.

12.26 Several stakeholders supported this proposal.[28] The ALRC would welcome further comment on the desirability and practicability of the proposal and the form and content of the proposed provision.

12.27 The statutory tort for serious invasion of privacy proposed in this Discussion Paper itself provides for a public interest balancing process.[29] In addition to this, the statute could further provide that courts must have particular regard to freedom of expression, when considering whether to grant injunctive relief. The experience in the United Kingdom, as discussed later in this chapter, would be relevant to the function and desirability of such a provision.

12.28 However, this proposal would arguably be of particular benefit, on its own, if the statutory cause of action is *not* enacted. As set out below, there is some uncertainty as to the approach that a court should take to applications for injunctive relief in some cases. The question is whether it would be desirable for legislation to direct or guide the approach that the courts should take.

12.29 This may be justified to promote not only coherence but also the balancing of freedom of expression and other public interests with privacy protection. The following sections set out the complex legal principles and issues that underpin this proposal.

12.30 In a privacy case, perhaps even more so than in other cases such as cases for defamation,[30] the stakes are high for both parties. Privacy in information, once lost,

---

28 RSPCA, *Submission 49*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; ABC, *Submission 46*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*; Pirate Party of Australia, *Submission 18*.

29 See Ch 8.

30 Defamation is essentially concerned with *false* and derogatory statements: David Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy' (2012) 17 *Media & Arts Law Review* 170. The distinction may not be clear cut: damage to reputation may be difficult to repair, and some false slurs will inevitably leave a residual doubt in people's minds, so that the harm is in fact irreparable: *Hill v Church of Scientology of Toronto* (1995) 2 SCR 1130, [166]. However, many false statements of 'fact' can be proved to be false.

may be lost forever,[31] and no amount of compensation will render the information entirely private again.[32] Equally, by the time the entitlement of the defendant to publish is adjudicated in a final hearing, the appropriate opportunity to reveal the relevant information or contribute to a public debate may be lost as the information's novelty, relevance or interest is overtaken by other events.

12.31 As with all court orders, the ultimate efficacy of an injunction will depend on the jurisdiction of the court over the apprehended conduct, as well as the location of the respondent. The court will not grant an injunction where it would be futile to do so, and one ground for futility may be the wide publicity already given to the relevant information.[33]

12.32 According to equitable principles, as set out by the High Court of Australia in *Beecham Group v Bristol Laboratories Pty Ltd*[34] and reaffirmed in *ABC v O'Neill*,[35] before the court will exercise its discretion to award an interlocutory injunction, an applicant must satisfy the court that:

- there is a prima facie case, in the sense that there is a serious question to be tried as to the plaintiff's entitlement to relief, and a sufficient[36] likelihood of success to justify the preservation of the status quo pending trial;

---

31 *Prince Albert v Strange* (1849) 1 Mac & G 25, 46 (Lord Cottenham): 'In the present case, where privacy is the right invaded, postponing the injunction would be equivalent to denying it altogether.' See also *Tchenguiz v Imerman* [2010] EWCA (Civ) 908, [54] (Lord Neuberger MR). Lord Nicholls made the same point as to confidentiality in *Cream Holdings Ltd v Banerjee* (2004) 1 AC 253, [18]. See also Eric Barendt, *Freedom of Speech* (Oxford University Press, 2nd ed, 2007) 136.

32 The court may, however, decide that damages would be an adequate remedy, and thus, on the threshold equitable test, refuse the injunction: see *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457, where Young J refused the plaintiff's claim for an injunction to restrain the broadcast of footage obtained while trespassing on this ground, obviating the need to consider public interest.

33 *Candy v Bauer Media Limited* [2013] NSWSC 979, [20]; *Mosley v News Group Newspapers* [2008] EWHC 687 (QB), [36]. See Normann Witzleb, '"Equity Does Not Act in Vain": An Analysis of Futility Arguments in Claims for Injunctions' (2010) 32 *Sydney Law Review* 503. A related question of fact is whether, for the purposes of the equitable obligation, the information had the quality of confidence or whether it is at the relevant time in the public domain. Where publication is not widespread, there may still be some point to restricting further publication: *Johns v Australian Securities Commission* (1993) 178 CLR 408, [460]–[462] (Gaudron J); *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [428]–[429]; *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109. Contractual obligations of confidence raise different considerations: see *Massingham v Shamin* [2012] NSWSC 288 (23 March 2012) and cases referred to therein.

34 *Beecham Group v Bristol Laboratories Pty Ltd* (1968) 118 CLR 618.

35 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57. See further David Rolph, 'Showing Restraint: Interlocutory Injunctions in Defamation Cases' (2009) 14 *Media & Arts Law Review* 255; Benedict Bartl and Dianne Nicol, 'The Grant of Interlocutory Injunctions in Defamation Cases in Australia Following the Decision in Australian Broadcasting Corporation v O'Neill' (2006) 25 *University of Tasmania Law Review* 156.

36 'The requisite strength of the probability of ultimate success depends upon the nature of the rights asserted and the practical consequences likely to flow from the interlocutory order sought… [such as the fact that] the grant or refusal of the interlocutory application would dispose of the action finally': *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [71]-[72] (Gummow and Hayne JJ).

- the plaintiff is likely to suffer injury for which damages will not be an adequate remedy;[37] and
- the balance of convenience favours the granting of an injunction.[38]

Injunctions in defamation and breach of confidence

12.33 Applications for injunctive relief to restrain publication are commonly made in defamation and breach of confidence cases.

12.34 In actions for defamation, an applicant faces additional hurdles to those set out in *Beecham,* when seeking an interlocutory injunction. The so-called rule in *Bonnard v Perryman* is derived from Lord Coleridge CJ's statement in that case 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'.[39] In particular, if a defendant asserts that it will defend the defamatory statement as true, then, 'in all but exceptional cases',[40] the courts will exercise their discretion to refuse the injunction, leaving the defendant to publish and risk liability for damages.

12.35 This caution in defamation cases is well-established in Australian law, although the defendant must go further than merely *raising* the defence.[41] 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.[42] Gummow and Hayne JJ referred to the need for the judge to consider 'the … general and … profound issue involved in the policy of the law respecting prior restraint of publication of allegedly defamatory matter'.[43]

12.36 Gummow and Hayne JJ also emphasised that claims for interlocutory injunctions in defamation in Australia, although reflecting the principle in *Bonnard*, are 'but one of a species of litigation to which the principles in *Beecham* apply'.[44] That

---

37 This second factor is not necessary if the application is in the exclusive equitable jurisdiction of the court, for example to restrain the breach of an equitable duty of confidence: Meagher, Heydon and Leeming, above n 18, [21–345].

38 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [19] (Gleeson CJ and Crennan J); Ibid, [65]–[72] (Gummow and Hayne JJ).

39 *Bonnard v Perryman* [1891] 2 Ch 269, 283-285. Gummow and Hayne JJ point out in *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [80] that the court in *Fleming v Newton* [1848] 9 ER 797 was wary both of usurping the role of the jury at trial and of constraining the liberty of the press after the lapsing of a statutory system of press licensing.

40 *Bonnard v Perryman* (1891) 2 Ch 269, 285.

41 *National Mutual Life Association of Australasia Ltd v GTV Corpn Pty Ltd* [1989] VR 747; *Chappell v TCN Channel Nine Pty Ltd* (1988) 14 NSWLR 153; *Clarke v Queensland Newspapers Pty Ltd* [2000] 1 Qd R 233; *Jakudo Pty Ltd v South Australian Telecasters Ltd* (1997) 69 SASR 440, [442]–[443].

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

43 *Australian Broadcasting Corporation v O'Neill* (2006) has been applied in several cases: *AAMAC Warehousing & Transport Pty Limited v Fairfax Media Publications Pty Limited* [2009] NSWSC 1030 (28 September 2009); *Crisp v Fairfax Media Ltd* [2012] VSC 615 (19 December 2012); *Allan v The Migration Institute of Australia Ltd* [2012] NSWSC 965 (13 August 2012); cf *Tate v Duncan-Strelec* [2013] NSWSC 1446 (27 September 2013).

44 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [75].

broader species includes cases where the disposal of the interlocutory application would effectively determine the case in its entirety, but also, presumably, applications for interlocutory injunctions in the auxiliary jurisdiction in general.

12.37 In direct contrast to defamation cases, courts considering injunctions to restrain a breach of confidence do not exercise any special caution in the interests of free speech or other broadly defined public interests. Both in claims for breach of an *equitable* obligation of confidence, which lie in equity's exclusive jurisdiction,[45] and perhaps even more so in claims to restrain the breach of a *contractual* obligation of confidence,[46] which lie in the auxiliary jurisdiction,[47] authority in Australia takes a narrow approach to public interest considerations that would justify a breach.

12.38 The principle of general application, where the court is considering an injunction to restrain the breach of an equitable obligation of confidence, was stated by Gummow J in *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd*:

> That principle, in my view, is no wider than one that information will lack the necessary attribute of confidence if the subject matter is the existence or real likelihood of the existence of an iniquity in the sense of a crime, civil wrong or serious misdeed of public importance, and the confidence is relied upon to prevent disclosure to a third party with a real and direct interest in redressing such crime, wrong or misdeed.[48]

12.39 The current Australian approach differs from the much broader approach to public interest taken in the United Kingdom in such cases.[49] In a later case, Gummow J stated:

> (i) an examination of the recent English decisions shows that the so-called 'public interest' defence is not so much a rule of law as an invitation to judicial idiosyncrasy by deciding each case on an ad hoc basis as to whether, on the facts overall, it is better to respect or to override the obligation of confidence, and (ii) equitable principles are best developed by reference to what conscionable behaviour demands of the

45 The exclusive jurisdiction arises where a court of equity is dealing with equitable claims: Meagher, Heydon and Leeming, above n 18, [21–015].

46 *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987) [57].

47 The auxiliary jurisdiction of equity arises where the court is considering equitable remedies in aid of common law wrongs or to prevent the unconscionable reliance on common law rights: Meagher, Heydon and Leeming, above n 18, [21–345].

48 *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987) [57].

49 *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [72]–[94]; *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987), [41]; *AG Australia Holdings Ltd v Burton* 58 NSWLR 464, [173]; Meagher, Heydon and Leeming, above n 18, [41–115]–[41–125]. Cf Aplin et al, above n 19, [16.05]–[16.57] on the more recent, more expansive approach.

> defendant not by balancing and then overriding those demands by reference to matters of social or political opinion.[50]

12.40 More recently, it has been said that '[i]t is true that the existence of, and /or the extent of any public interest defence to a breach of confidentiality is by no means clear and settled in Australia'.[51]

Injunctions to restrain disclosure of *private* information

12.41 Questions then arise as to what approach the courts should take, in the absence of a statutory cause of action for invasion of privacy, where they are considering a claim for misuse or disclosure of *private* (rather than confidential) information.[52] Should 'private information' cases be seen as more analogous to defamation cases or as more analogous to traditional breach of confidence cases? Should a similar caution as in defamation cases be exercised when considering applications for interlocutory injunctions to restrain publication of private information?

12.42 In many cases where there is a potential for inconsistency between different causes of action, or between common law and statutory regimes, the High Court of Australia has emphasised the need for coherence in the development of the common law.[53]

12.43 Although they may overlap, or arise concurrently, cases involving the apprehended disclosure of private information raise somewhat different issues from apprehended defamation cases. Unlike in a defamation case, a defendant in a privacy case cannot assert the truth of the disclosed information as a defence.[54] There is, however, just as strong and justifiable a concern that undue restrictions upon freedom of speech and the freedom of the press might arise from unmeritorious claims to prevent the disclosure of allegedly 'private' information in which there is a legitimate public interest. It is therefore strongly arguable that similar considerations to those in defamation cases should apply where the defendant asserts a defence of sufficient strength to justify the court taking a cautious approach.[55] The ALRC proposal reflects

---

50 *Smith Kline and French Laboratories (Aust) Ltd v Secretary, Dept of Community Services and Health* [1990] FCR 73, 111. See further, *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [72]–[94].

51 *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [75].

52 *Spelman v Express Newspapers* [2012] EWHC 355 (QB) (24 February 2012), [64]: 'There is some uncertainty as to whether, and if so when, a court should refuse an injunction on the basis of *Bonnard v Perryman* when it is sought by a claimant who advances his cases only on the basis of privacy'.

53 *Sullivan v Moody* (2001) 207 CLR 562. See further, Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy', above n 29, 187-190; Tilbury, above n 7, 130 ff.

54 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: C Sappideen and P Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) 635–639.

55 There is also a concern that, if the applicable considerations or approach to be applied by the courts in defamation cases and privacy cases differed, a claimant may attempt to avoid the cautious approach in defamation cases, by framing or pleading his or her case, inappropriately, as a privacy case: *Lord Browne*

that concern, and suggests that the courts should be directed to consider countervailing public interests when dealing with an application for an injunction to restrain the publication of *private* information.

12.44 To avoid dispute and ensure consistency, any guidance by legislation should apply expressly to *any* action to prevent publication of information on the basis that it is private (rather than confidential) information. The key point is that, whether the legal protection of private information at common law in the future takes the form of a new tort or an extended action for breach of confidence, the court should be required to consider and weigh any countervailing public interests, such as freedom of expression, in its disclosure. This should apply regardless of whether the court is exercising its exclusive or auxiliary jurisdiction.

12.45 The ALRC's proposal has a similar intent to the provisions in s 12(4) of the *Human Rights Act 1998* (UK), although it is in more general terms. That provision reflects the concern that injunction applications in privacy actions may have a chilling effect on freedom of speech. Section 12(4) reinforces the requirement of the *European Convention on Human Rights* that the right to privacy in art 8 be balanced with the right to freedom of expression in art 10, when determining whether there has been an actionable invasion of privacy at all. While this balancing already takes place when determining whether there is an actionable misuse of private information,[56] s 12 provides added protection of art 10 rights:[57]

> s 12 Freedom of expression
>
> 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

---

of Madingly v Associated Newspapers Ltd [2007] EWHC 202 (QB), [28] (Eady J). This concern motivated Tugendhat J in *Terry v Persons Unknown* [2010] EWHC 202 (QB) to note at [88] that 'it is a matter for the court to decide whether the principle of free speech prevails or not, and that it does not depend solely upon the choice of the claimant as to his cause of action'. He dismissed the claimant's application for an injunction to restrain the publication of confidential and private information, at [123]: 'Having decided that the nub of this application is a desire to protect what is in substance reputation, it follows that in accordance with *Bonnard v Perryman* no injunction should be granted'. Witzleb argues that this approach is inconsistent with the requirements of the *Human Rights Act 1998* (UK); N Witzleb, 'Interim Injunctions for Invasions of Privacy: Challenging the Rule in Bonnard v Perryman?' in N Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014). Cf Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy', above n 29, on the Australian position.

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

57 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.

(ii) it is, or would be, in the public interest for the material to be published;

(b) any relevant privacy code.

12.46 Section 12(4) of the *Human Rights Act 1998* (UK) has been considered in a number of cases since its enactment and by a Joint Committee of the House of Lords and House of Commons in 2012. The courts rejected an interpretation that the sub-section requires them to give *greater* weight to the Convention rights to freedom of expression than to the plaintiff's interest in privacy. Lord Hope in *Campbell v MGN Ltd*:

> [A]s Sedley LJ said in *Douglas v Hello! Ltd* you cannot have particular regard to article 10 without having equally particular regard at the very least to article 8: see also *Re S (A Child) (Identification: Restrictions on Publication)* where Hale LJ said that section 12(4) does not give either article pre-eminence over the other. These observations seem to me to be entirely consistent with the jurisprudence of the European court.[58]

12.47 The House of Lords and House of Commons Joint Committee's Report stated:

> We do not think that section 12(4) of the *Human Rights Act 1998* ... means that article 10 has precedence over article 8 ... However, we support the decision of Parliament to make clear in law the fundamental importance of freedom of expression and would be concerned that removing section 12(4) might suggest that this is no longer the case.[59]

12.48 In the light of well-established principles concerning ex parte applications,[60] and the strength of the defendant's case in interlocutory proceedings,[61] it is not suggested that provisions similar to subsections (2) and (3) of s 12 of the *Human Rights Act* (UK) are necessary or desirable in Australia.[62]

---

58 *Campbell v MGN Ltd* [2004] 2 AC 457, [488] (citations omitted).

59 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), [59]. David Price QC was quoted at [58] as having told the committee: 'If the purpose of section 12 was to give the benefit of the doubt to freedom of expression then it has certainly failed'. Professor Gavin Phillipson of Durham Law School, quoted at [55], considered that s 12(4) was not intended 'to establish priority for freedom of expression ... [and] it made more sense to read it as requiring judges to give as much weight to freedom of expression as the Convention itself allows'.

60 See further, Meagher, Heydon and Leeming, above n 18, [21–425].

61 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57; *Beecham Group v Bristol Laboratories Pty Ltd* (1968) 118 CLR 618.

62 Section 12(2) and (3) of the *Human Rights Act 1998* (UK) provides: '(2) If the person against whom the application for relief is made (the respondent) is neither present nor represented, no such relief is to be granted unless the court is satisfied—(a) that the applicant has taken all practicable steps to notify the respondent; or (b) that there are compelling reasons why the respondent should not be notified. (3) No such relief is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is likely to establish that publication should not be allowed'. On the meaning of 'likely' in subsection (3), see *Cream Holdings Ltd v Banerjee* (2004) 1 AC 253 where Lord Nicholls stressed at [22] that 'likely' could mean different things depending upon its context; *ETK v News Group Newspapers Ltd* [2011] EWCA Civ 439 (19 April 2011), [6], [24]: '...likely in the sense of more likely than not'.

12.49 It should also be noted that this proposal is not intended to affect the existing law with regard to applications for injunctions to restrain the breach of an equitable or contractual obligation of confidence As explained above, particular considerations apply to the justification for a disclosure by a confidant in breach of a pre-existing obligation or by a third party who has knowledge that the information was imparted in confidence,[63] where the law, for reasons of public interest, seeks to uphold and reinforce the obligation undertaken. Arguably, different considerations should apply, when there is no such obligation as the foundation for the plaintiff's application, but the plaintiff relies merely on the nature of the information itself and the reasonable expectation of privacy that arises from the particular circumstances. In such cases, it is appropriate that greater weight be given to countervailing interests and matters of public interests.

63 Meagher, Heydon and Leeming, above n 18, [41–115]-[41–125]. See further, *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [72]-[94]; *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987), [41]. Cf Aplin et al, above n 19, [16.05]–[16.57] on the recent more expansive English approach.

13. Surveillance Devices

Contents

Summary

13.1 In this chapter, the ALRC proposes that surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.

13.2 Existing surveillance device laws in each state and territory provide criminal offences for the unauthorised use of listening devices, optical surveillance devices, tracking devices, and data surveillance devices. These surveillance device laws provide important privacy protection by creating offences for unauthorised surveillance.

13.3 However, there is significant inconsistency between the laws with respect to the types of devices regulated and with respect to the offences, defences and exceptions. This inconsistency results in reduced privacy protections for individuals, and increased uncertainty and compliance burdens for organisations.

13.4 Additionally, the ALRC proposes that surveillance device laws make provision for courts to award compensation to victims of breaches of surveillance device laws. The ALRC has also asked whether local councils should be empowered to regulate the use of surveillance devices in some circumstances. Council regulation may be more appropriate for less serious uses of surveillance devices.

Uniform surveillance laws

Proposal 13–1 Surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.

Proposal 13–2 Surveillance device laws should include a technology neutral definition of 'surveillance device'.

Proposal 13–3 Offences in surveillance device laws should include an offence proscribing the surveillance or recording of private conversations or activities without the consent of the participants. This offence should apply regardless of whether the person carrying out the surveillance is a participant to the conversation or activity, and regardless of whether the monitoring or recording takes place on private property.

Proposal 13–4 Defences in surveillance device laws should include a defence of responsible journalism, for surveillance in some limited circumstances by journalists investigating matters of public concern and importance, such as corruption.

Question 13–1 Should the states and territories enact uniform surveillance laws or should the Commonwealth legislate to cover the field?

13.5 Surveillance device laws provide an important protection of privacy. Notably, the legislation offers some protection against intrusion into seclusion. Consistency in these laws is important both for protecting individuals' privacy and for reducing the compliance burden on organisations that use surveillance devices in multiple jurisdictions.

13.6 Protection from surveillance is a fundamental form of protection of privacy, particularly in the digital era. One US judge has described the impact of surveillance on privacy:

> What the ancients knew as 'eavesdropping' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb. Electronic surveillance is the greatest leveller of human privacy ever known.[1]

13.7 Surveillance laws protect other freedoms as well. Unauthorised surveillance may interfere with freedom of speech, freedom of movement and freedom of association.

13.8 Laws exist in each state and territory to regulate the use of surveillance devices.[2] These laws provide criminal offences for the unauthorised installation, use or

---

1 Douglas J of the Supreme Court (United States of America) as cited in *Miller v TCN Channel Nine* (1988) 36 Crim R 92, 94 (Finlay J).

2 *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). At the Commonwealth level, the *Surveillance Devices Act 2004* (Cth) makes provisions for the use of

maintenance of surveillance devices to record private conversations and private activities.[3] Other laws in the ACT, NSW and Victoria regulate the use of surveillance in the workplace.

13.9 These surveillance device and workplace surveillance laws contain a number of significant inconsistencies across jurisdictions. These inconsistencies fall broadly into three categories. There are inconsistencies with respect to:

- the type of the devices regulated;
- the nature of the offences; and
- the nature of the defences and exceptions.

13.10 Consistency and uniformity in the surveillance device laws and workplace surveillance laws is desirable. Inconsistency means that privacy protections vary depending on which state or territory a person is located in. It also makes it more difficult for a person who finds themselves under surveillance to determine their legal position. Inconsistency also means that organisations with legitimate uses for surveillance devices face increased uncertainty and regulatory burden. Many stakeholders agreed that uniformity was desirable.[4] The ALRC discussed the benefits of uniformity in its 2008 report, 'For your information: Australian privacy law and practice'.[5]

13.11 The ALRC has proposed that definitions, offences, prohibitions, defences and exceptions be made uniform across Australian states and territories. This proposal applies both to surveillance device laws and to workplace surveillance laws.

13.12 The ALRC has not proposed a particular process for achieving uniformity. It may be appropriate for the Commonwealth to introduce new legislation, possibly through the introduction of a Commonwealth Act that covers the field, replacing state and territory surveillance device laws. Any such Commonwealth legislation would likely engage the external affairs power of the Australian *Constitution*, as a means of giving effect to Australia's obligation under art 17 of the *International Covenant on Civil and Political Rights* to protect privacy.[6] Alternatively, a new Act may be supported by s 51(v) if it is characterised as regulating 'postal, telegraphic, telephonic,

---

surveillance devices by federal law enforcement officers, however it does not provide for offences applicable to general members of the public.

3 Other laws provide related protections, without necessarily being designed to control the use of surveillance devices per se. For example, s 227A of the Queensland *Criminal Code* provides for a misdemeanour where a person observes or visually records another person 'in circumstances where a reasonable adult would expect to be afforded privacy', if the second person is in a private place or engaged in a private act and has not provided consent. A similar offence exists in s 91K of the *Crimes Act 1900* (NSW), where the recording is obtained for the purpose of obtaining 'sexual arousal or sexual gratification'. While a surveillance device could be used in a way that contravened one of these laws, surveillance may occur in other situations. Surveillance is also included as a form of stalking in, eg, s 21A(f) of the *Crimes Act 1958* (Vic).

4 M Paterson, *Submission 60*; Free TV, *Submission 55*; Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; Australian Industry Group, *Submission 38*; Law Institute of Victoria, *Submission 22*; D Butler, *Submission 10*.

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) ch 3.

6 The external affairs power and the ICCPR are discussed further in Ch 4.

and other like services'. A Commonwealth Act that covered the field would exist alongside other Commonwealth privacy protections under the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth). The ALRC has asked whether it would be preferable to enact a Commonwealth law to replace state and territory surveillance device laws, rather than attempting to achieve uniformity in state and territory laws.

A technology-neutral definition of 'surveillance device'

13.13 Uniform surveillance device laws should adopt a technology-neutral definition of 'surveillance device' to ensure that the definition can be applied to a wide range of surveillance devices, including surveillance devices that emerge in the future. The definition should also extend to forms of surveillance that are not 'devices', such as data surveillance by software installed on a person's computer.[7]

13.14 This element of the ALRC's proposal would address the inconsistencies in the types of devices regulated under the existing surveillance device laws. Four types of devices are recognised in at least one surveillance device law: listening devices, optical surveillance devices, data surveillance devices and tracking devices. However:

- optical surveillance devices are not regulated by the surveillance device laws of the ACT, Queensland, SA or Tasmania;
- data surveillance devices are not regulated by the surveillance device laws of the ACT, Queensland, SA, Tasmania, or WA, and are only regulated by the Victorian and NT surveillance device laws when used, installed or maintained by law enforcement officers; and
- tracking devices are not regulated by the surveillance device laws of the ACT, Queensland, SA, or Tasmania.

13.15 Even where two jurisdictions regulate similar devices, there are some inconsistencies in the definition of those devices.

13.16 In NSW, for instance, a tracking device is defined as 'any electronic device capable of being used to determine or monitor the geographical location of a person or an object',[8] while in Victoria, the definition is 'an electronic device the primary purpose of which is to determine the geographical location of a person or an object'.[9] Many general-purpose devices—in particular, mobile phones—can also be used to determine location, despite this not being the primary purpose of the device. This difference in definition may therefore have a significant impact on the types of surveillance that are regulated in each state.

13.17 In a 2001 interim report, the NSWLRC proposed defining 'surveillance device' as 'any instrument, apparatus or equipment used either alone, or in conjunction with

---

7 *R v Gittany (No 5)* [2014] NSWSC 49 (11 February 2014) [7].
8 *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of 'tracking device').
9 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'tracking device').

other equipment, which is being used to conduct surveillance'.[10] The NSWLRC also proposed defining 'surveillance' as 'the use of a surveillance device in circumstances where there is a deliberate intention to monitor a person, a group of people, a place or an object for the purpose of obtaining information about a person who is the subject of the surveillance'.[11]

13.18 The regulation of several types of surveillance devices are discussed below. The ALRC welcomes comments from stakeholders on the appropriateness of regulating these or other types of surveillance devices.

Drones and mobile surveillance devices

13.19 The use of unmanned aerial vehicles (drones) to carry surveillance devices has generated some concern within Australia and internationally.[12] Although a drone by itself may not be a surveillance device, other devices attached to a drone (such as microphones or video cameras) may be.

13.20 The OAIC noted community concerns about drones in its 2012–13 annual report.[13] At the time of writing, the House of Representatives Standing Committee on Social Policy and Legal Affairs is conducting an inquiry into the use of drones.[14]

13.21 The ALRC has also received a number of submissions relating to drones. Some stakeholders noted, in general terms, the privacy issues relating to the use of drones.[15] Others commented on the use of drones to monitor activity taking place on farms.[16]

Wearable devices

13.22 Wearable devices, such as head-mounted cameras, have also generated public discussion. A notable example is Google's 'Glass' technology, a wearable device that includes video and audio recording capabilities. Several stakeholders noted the privacy challenges presented by such devices.[17]

13.23 Wearable devices with audio recording capabilities would typically fall within the definition of 'listening device' in each of the surveillance device laws. Similarly, wearable devices with optical recording capabilities would typically fall within the

---

10 NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) Rec 1.
11 Ibid Rec 2.
12 See, for example, 'Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft' (American Civil Liberties Union, December 2011).
13 Office of the Australian Information Commissioner, *Annual Report* (2012), xv.
14 House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, Inquiry into a matter arising from the 2012-13 Annual Report of the Office of the Australian Information Commissioner, namely the regulation of Unmanned Aerial Vehicles (2013).
15 Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Australian Privacy Foundation, *Submission 39*; Office of the Information Commissioner, Queensland, *Submission 20*.
16 Barristers Animal Welfare Panel and Voiceless, *Submission 64*; National Farmers' Federation, *Submission 62*; RSPCA, *Submission 49*; Australian Lot Feeders' Association, *Submission 14*.
17 Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; D Butler, *Submission 10*; P Wragg, *Submission 4*.

definition of 'optical surveillance device' in those laws that contain such a definition. However, several jurisdictions do not regulate optical surveillance devices.

13.24 It is important to note that uniform surveillance device laws would not, and should not, prohibit the use of such devices generally. A wearable device may have many legitimate uses that do not amount to surveillance. Whether or not the use of a device constituted an offence would depend on the circumstances of its use, such as the activity being captured, the extent of the monitoring or recording, and whether or not parties to the activity were aware that the device was being used.

Data surveillance devices

13.25 Surveillance device laws generally do not regulate phone tapping and other types of data or communications surveillance. Communications surveillance is regulated under the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act). Although the distinction between the two types of surveillance may become less clear as communication technologies continue to develop, the High Court has established that the TIA Act 'covers the field' of communications surveillance.[18]

13.26 Some surveillance device laws regulate some types of data surveillance—for example, devices that capture data by recording a person's keystrokes on a computer.[19] Other types of data surveillance may not be regulated under either surveillance device laws or the TIA Act. For example, information being transmitted over a radiocommunication system such as a wireless local network (wi-fi) appears to be excluded from the protections of the TIA Act[20] and may also fall outside existing definitions of 'data surveillance device'. Also, as noted in a submission from Associate Professor Moira Paterson,[21] radio frequency identification (RFID) devices such as electronic door key cards or passports are capable of transmitting information, and should also be protected from surveillance.

13.27 These types of data surveillance would need to be considered in drafting new uniform surveillance device laws.

Tracking devices

13.28 At present, tracking devices are regulated in only a few Australian jurisdictions. The definition of 'tracking device' is not consistent among these jurisdictions. Uniform surveillance device laws should address this inconsistency and ensure that tracking devices are regulated across Australia.

13.29 Consideration should also be given to regulating methods of tracking that do not rely on a tracking device being carried by the individual, but instead make use of a network of devices to determine the individual's location.[22] This could include, for

---

18 *Miller v Miller* (1978) 141 CLR 269.

19 See, eg, *Surveillance Devices Act* (NT) s 4 (definition of 'data surveillance device').

20 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5 (definitions of 'telecommunications network' and 'telecommunications service').

21 M Paterson, *Submission 60*.

22 Ibid; Electronic Frontiers Australia, *Submission 44*.

example, a communications network being used to determine the location of an individual's mobile phone, even where the mobile phone does not provide location information directly.[23]

Uniform offences

13.30 The ALRC proposes establishing uniform offences for the use of surveillance devices to monitor 'private activities' (however defined). The protection of privacy of individuals within Australia should not depend on the state or territory where the individual is located. One important step towards achieving uniformity would be ensuring that a given activity receives the same protection from surveillance regardless of the jurisdiction in which it occurs. To that end, a uniform definition of 'private activity' could be adopted.[24] This would be in keeping with the largely uniform definitions of 'private conversation' that apply in each jurisdiction for the purposes of the offence for surveillance using a listening device.

13.31 Each of the surveillance device laws provides a number of offences. These offences include, for example, offences for carrying out surveillance, offences for communicating information obtained by surveillance,[25] and offences for providing surveillance devices for sale.[26]

13.32 This chapter is concerned with the first of these types of offence—offences for carrying out surveillance.[27] The nature of these surveillance offences under existing surveillance device laws differ across jurisdictions. Each jurisdiction has an offence of carrying out surveillance of a private conversation using a listening device.[28] However, the offences with respect to other types of devices are inconsistent. For example:

- the offence for optical surveillance of a private activity in Victoria does not apply to activities carried on outside a building—optical surveillance of activities in a person back yard, for example, are permitted under the Victorian Act;[29]

---

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

24 An alternative approach would be to follow the NSW Act and define the offences in terms of interference with property rather than by reference to the nature of the conversation or activity under surveillance: *Surveillance Devices Act 2007* (NSW) s 8.

25 Eg, *Surveillance Devices Act 1999* (Vic) ss 11, 12; *Surveillance Devices Act* (NT) ss 15, 16.

26 *Surveillance Devices Act 2007* (NSW) s 13.

27 This is not to say that there are no inconsistencies in the other types of offences. However, the offences for carrying out surveillance are the primary protections of privacy in these laws, and so removing the inconsistencies in these offences is a priority.

28 Eg, *Surveillance Devices Act 1998* (WA) s 5; *Listening and Surveillance Devices Act 1972* (SA) s 4; *Invasion of Privacy Act 1971* (Qld) s 43.

29 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'private activity'). The Victorian Law Reform Commission has previously recommended removing the exception for activities carried on outside a building; see Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 11.

- the offences for optical and data surveillance in NSW do not depend on the nature of the activity or information placed under surveillance, but only on whether the installation, use or maintenance of the surveillance device required entry onto premises or interference with a car, computer or other object;[30] and
- the offences for data surveillance in Victoria and the NT provide a more general offence for using a data surveillance device to monitor information input to, or output from, a computer system, but these offences only apply to law enforcement officers.[31]

13.33 Differences also exist between the surveillance device laws with respect to the fault element in the offences for installing, using or maintaining a surveillance device. For example:

- the offence for the use of a listening device under the *Listening and Surveillance Devices Act 1972* (SA) requires intentional use of the device;[32]
- the offence for the use of a listening device under the *Invasion of Privacy Act 1971* (Qld) does not require intent,[33] although an exception applies for the 'unintentional hearing of a private conversation by means of a telephone';[34] and
- the offence for the use of a listening device under the *Listening Devices Act 1991* (Tas) includes an exception for 'the unintentional hearing of a private conversation by means of a listening device'[35]—not just for unintentional hearing by means of a telephone, as in the Queensland law.

13.34 There are other inconsistencies in the surveillance device laws with regard to other offences, such as the communication of information obtained through prohibited surveillance. In order to ensure uniformity between the surveillance device laws, such inconsistencies would need to be removed as well. However, these other offences are largely dependent on the general offences (for installing, using, or maintaining surveillance devices) considered above. Achieving uniformity in these more general offences is therefore a prerequisite for obtaining uniformity in the remaining offences.

Uniform defences and exceptions

13.35 As well as uniform offences, the surveillance device laws of each state and territory should, as far as possible, provide for uniform defences and exceptions.[36]

13.36 Many state and territory surveillance device laws contain a number of broadly similar exceptions to the offence of using, installing or maintaining a surveillance device. All jurisdictions permit surveillance in accordance with a warrant or other

30 *Surveillance Devices Act 2007* (NSW) ss 8, 10.
31 *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9.
32 *Listening and Surveillance Devices Act 1972* (SA) s 4.
33 *Invasion of Privacy Act 1971* (Qld) s 43(1).
34 Ibid s 43(2)(b).
35 *Listening Devices Act 1991* (Tas) s 5(2)(d).
36 The inconsistency of defences in existing surveillance device laws was noted by D Butler, *Submission 10*.

authorisation,[37] and all jurisdictions permit surveillance of a private conversation or activity if all the parties to the conversation or activity provide consent. Exceptions also exist for surveillance carried out in accordance with other legal requirements.[38]

13.37 One significant difference between the surveillance device laws relates to surveillance of a private conversation or activity by a party to that conversation or activity. Typically, an exception to a surveillance offence exists where all parties to the private conversation or activity provide consent.[39] However, in several jurisdictions, consent is not required if the person using, installing or maintaining the surveillance device is a party to the private activity or private conversation.[40]

13.38 The inconsistency with regard to this exception for participants means, for instance, that a journalist who records a conversation to which they are a party may have committed an offence in one jurisdiction, while the same recording would be permitted in another jurisdiction. The VLRC has referred to this exception for participants as a 'participant monitoring exception'.[41]

13.39 Other defences and exceptions also differ between jurisdictions:

- some jurisdictions provide an exception if the surveillance has the consent of all 'principal parties' to a conversation, being those parties that speak or are spoken to in a private conversation or who take part in a private activity;[42]
- some jurisdictions provide an exception if the surveillance has the consent of one principal party to a conversation and is reasonably necessary for the protection of a lawful interest of that principal party;[43]
- some jurisdictions provide an exception if the surveillance has the consent of one principal party and is not carried out for the purpose of communicating the

---

37 *Surveillance Devices Act 2007* (NSW) ss 7(2)(a), 8(2)(a), 9(2)(a), 10(2)(a); *Invasion of Privacy Act 1971* (Qld) s 43(2)(c); *Listening and Surveillance Devices Act 1972* (SA) s 6; *Listening Devices Act 1991* (Tas) s 5(2)(a); *Surveillance Devices Act 1999* (Vic) ss 6(2)(a), 7(2)(a), 8(2)(a), 9(2)(a); *Surveillance Devices Act 1998* (WA) ss 5(2)(a), 5(2)(b), 6(2)(a), 6(2)(b), 7(2)(b), 7(2)(c); *Listening Devices Act 1992* (ACT) s 4(2)(a); *Surveillance Devices Act* (NT) ss 11(2)(a), 12(2)(a), 13(2)(a), 14(2)(a).

38 Such requirements can be found, for example, in *Liquor Regulation 2008* (NSW) r 53H; *Transport (Taxi-Cab) Regulations 2005* (Vic) r 15.

39 See, for example, *Surveillance Devices Act 2007* (NSW) s 7(3); *Listening and Surveillance Devices Act 1972* (SA) s 4; *Surveillance Devices Act 1998* (WA) ss 5(3), 6(3). In some jurisdictions, it is sufficient that the 'principal parties' to the conversation or activity provide consent.

40 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1); *Invasion of Privacy Act 1971* (Qld) s 43(2)(a); *Surveillance Devices Act* (NT) ss 11(1)(a), 12(1)(a).

41 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [6.54]–[6.58].

42 *Listening Devices Act 1992* (ACT) s 4(3)(a); *Surveillance Devices Act 2007* (NSW) s 7(3)(a); *Listening Devices Act 1991* (Tas) s 5(3)(a); *Surveillance Devices Act 1998* (WA) ss 5(3)(c), 6(3)(a).

43 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening and Surveillance Devices Act 1972* (SA) s 7(1) (but note that this does not require that the person is a principal party, merely a party); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii).

recording, or a report of the recording, to anyone who was not a party to the conversation or activity;[44] and

- some jurisdictions provide an exception where the use of a surveillance device is in the public interest.[45]

13.40 The ALRC proposes that the defences and exceptions in the surveillance device laws be made consistent. In removing inconsistencies, it is necessary to decide which defences and exceptions should remain. The ABC expressed a concern that uniformity might be achieved by removing important defences and exceptions that allow for the use of surveillance devices in the public interest.[46] The ALRC has specifically proposed a defence for responsible journalism (discussed further below).

13.41 The ALRC also proposes that unified surveillance device laws do not include a participant monitoring exception. Removing this exception would provide greater privacy protections to individuals. Removing the exception would also provide greater freedom of expression to individuals, who would be able to take part in conversations and activities confident that no other participant was recording the event.

13.42 The VLRC similarly proposed removing the participant monitoring exception from the *Surveillance Device Law 1999* (Vic),[47] noting that:

> [i]t is strongly arguable that it is offensive in most circumstances to record a private conversation or activity to which a person is a party without informing the other participants.[48]

13.43 In the absence of the participant monitoring exceptions, certain other exceptions or defences may be appropriate. An exception may be appropriate where a person using surveillance is a party to a conversation or activity and the use of the surveillance is necessary for the protection of a lawful interest of that person. As noted earlier, this exception exists in other surveillance device laws,[49] but is redundant where a participant monitoring exception applies.

13.44 An exception should continue to apply where the consent of all parties had been obtained. Legitimate uses of surveillance devices (for example, to record a consumer's agreement to the terms of a contract over the phone) would therefore not be affected, provided consent was obtained.

---

44 *Listening Devices Act 1992* (ACT) s 4(3)(b)(ii); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(ii) (this exception is not available with respect to optical surveillance); *Listening Devices Act 1991* (Tas) s 5(3)(b)(ii).

45 *Surveillance Devices Act 1998* (WA) s 24 (definition of 'public interest'); *Surveillance Devices Act* (NT) s 41 (definition of 'public interest').

46 ABC, *Submission 46*.

47 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 18.

48 Ibid [6.57].

49 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening and Surveillance Devices Act 1972* (SA) s 7(1) (but note that this does not require that the person is a principal party, merely a party); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii).

13.45 Some legitimate uses of surveillance devices by journalists may place journalists at risk of committing an offence under existing surveillance device laws. Responsible journalism is an important public interest and should be protected. Journalists and media organisations should not be placed at risk of committing a criminal offence in carrying out legitimate journalistic activities. The ALRC has therefore proposed a 'responsible journalism' defence to surveillance device laws. This defence should be confined to responsible journalism involving the investigation of matters of public concern and importance, such as the exposure of corruption.

13.46 A number of other exceptions, as noted above, are already present in a number of the surveillance device laws. These exceptions should be considered in any process to make the surveillance device laws uniform.

Uniform workplace surveillance laws

13.47 Workplace surveillance legislation is also inconsistent across jurisdictions. Workplace surveillance laws recognise that employers are justified in monitoring workplaces for the purposes of protecting property, monitoring employee performance or ensuring employee health and safety. However, the interests of employers must be balanced against employees' reasonable expectations of privacy in the workplace. Specific workplace surveillance laws (the workplace surveillance laws) exist only in NSW,[50] the ACT[51] and, to some extent, in Victoria.[52] As with general surveillance device laws, uniformity about workplace surveillance laws would promote certainty, particularly for employers and employees located in multiple jurisdictions.

13.48 The *Surveillance Devices Act 1999* (Vic) provides an offence for the use of an optical device or listening device to carry out surveillance of the conversations or activities of workers in workplace toilets, washrooms, change rooms or lactation rooms.[53] Workplace surveillance in Victoria is otherwise subject to the same restrictions as general surveillance devices.

13.49 The *Workplace Privacy Act 2011* (ACT) applies to optical devices, tracking devices and data surveillance devices, but not to listening devices.[54] The Act requires an employer to provide particular forms of notice to employees if one of these types of surveillance devices is in use in the workplace, and to consult with employees in good faith before surveillance is introduced.[55] The Act also provides for 'covert surveillance authorities', allowing an employer to conduct surveillance without providing notice upon receiving an authority from a court. A covert surveillance authority will be issued only for the purpose of determining whether an employee is carrying out an unlawful activity, and is subject to various safeguards.[56] The ACT Act also prohibits

50 *Workplace Surveillance Act 2005* (NSW).
51 *Workplace Privacy Act 2011* (ACT).
52 *Surveillance Devices Act 1999* (Vic) pt 2A.
53 Ibid s 9B.
54 *Workplace Privacy Act 2011* (ACT) s 11(1) (definition of 'surveillance device').
55 Ibid pt 3.
56 Ibid pt 4.

surveillance of employees in places such as toilets, change rooms, nursing rooms, first-aid rooms and prayer rooms, and surveillance of employees outside the workplace.[57]

13.50 The *Workplace Surveillance Act 2005* (NSW) similarly applies only to 'optical surveillance', 'computer surveillance' and 'tracking surveillance'.[58] The NSW Act contains similar restrictions to those under the ACT Act. Surveillance devices must not be used in a workplace without sufficient notice being provided to employees,[59] must not be used in a change room, toilet, or shower facility,[60] and must not be used to conduct surveillance of the employee outside work.[61] Covert surveillance must not be used unless a covert surveillance authority is obtained.[62] The NSW Act also places limitations on the restriction of employee email and internet access while at work.[63]

13.51 The inconsistencies between these workplace surveillance laws are relatively minor—for example, slightly different definitions apply, and the types of rooms that may not be put under surveillance differ slightly between each law. A more significant need for reform arises because specific workplace surveillance laws exist only in these jurisdictions. The ALRC therefore proposes that there be uniform workplace surveillance laws across Australia.

13.52 Establishing uniform workplace surveillance laws in each of the states and territories would provide greater privacy protections for employees and greater certainty for employers operating in multiple jurisdictions. These laws could be contained in specific workplace surveillance laws, as they are in the ACT and NSW, or integrated into the more general surveillance device laws, as they are in Victoria.[64]

Compensation for victims of surveillance

Proposal 13–5 Surveillance device laws should provide that a court may make orders to compensate or otherwise provide remedial relief to a victim of unlawful surveillance.

13.53 Privacy protections afforded to individuals by the criminal law are limited in that the criminal law punishes the offender without necessarily providing redress to the

57 Ibid pt 5.

58 *Workplace Surveillance Act 2005* (NSW) s 3. The definition of 'tracking surveillance' refers to a device 'the primary purpose of which is to monitor or record geographical location or movement'. This is arguably another inconsistency in surveillance laws. The definition of 'tracking device' in s 4 of the *Surveillance Devices Act 2007* (NSW) does not require that tracking be the primary purpose of the device, but the definition of 'tracking device' in s 3 of the *Workplace Surveillance Act 2005* (NSW) does require that tracking be the primary purpose.

59 Ibid pt 2.

60 Ibid s 15.

61 Ibid s 16. An exception applies where the surveillance is computer surveillance on equipment provided at the employer's expense.

62 Ibid pt 4.

63 Ibid s 17.

64 The latter, integrated approach was recommended by the NSWLRC: NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) Rec 57.

victim. While an individual who has been subjected to unlawful surveillance may gain some satisfaction from seeing the offender fined, and while the fine may dissuade the offender from conducting further unlawful surveillance in the future, the victim will generally not receive any compensation or other personal remedy.

13.54 If uniform surveillance device laws are introduced through reforms to existing state and territory legislation, a provision allowing for compensation to victims would operate alongside compensation provisions already provided for by existing state and territory legislation.[65] However, providing for compensation within the uniform surveillance device laws would ensure that uniform compensation mechanisms existed for victims of unlawful surveillance.

13.55 All states and territories have established victims' compensation schemes that provide for compensation to be paid to victims of crimes.[66] Unlike an order for compensation to be paid by an offender, a victims' compensation scheme does not depend on an offender's ability to pay the compensation. However, victims' compensation schemes are generally available only for serious physical crimes such as assault, robbery, or sexual assault,[67] and surveillance is therefore unlikely to give rise to compensation under these schemes.

13.56 The ALRC proposes that the surveillance device laws of the states and territories—whether made uniform or not—should allow courts to order compensation be paid to individuals who are victims of unlawful surveillance. Such a change to surveillance device laws was suggested by Professor Des Butler, who submitted that the laws 'should in addition make provision for recovery of compensation or other remedies such as injunction by any aggrieved person'.[68]

13.57 Mechanisms for compensation can be found in other, analogous, criminal laws. Remedial relief is available, for example, under s 107A of the *Telecommunications (Interception and Access) Act 1997* (Cth). Under this section, an aggrieved individual may apply to the court for remedial relief if a defendant is convicted of intercepting or communicating the contents of a communication.[69]

---

65 Courts may order compensation for loss, injury or damage under, for example, *Crimes (Sentencing) Act 2005* (ACT) s 18; *Criminal Law (Sentencing) Act 1988* (SA) s 53; *Sentencing Act 1991* (Vic) s 85B; *Victims Rights and Support Act 2013* (NSW) ss 91–103.

66 For a general discussion of these schemes, see Australian Law Reform Commission and NSW Law Reform Commission, *Family Violence: A National Legal Response*, ALRC Report No 114, NSWLRC Report 128 (October 2010) ch 4.

67 *Victims Rights and Support Act 2013* (NSW) s 5; *Victims of Crime Assistance Act 1996* (Vic) ss 7–13.

68 D Butler, *Submission 10*.

69 The remedies available under this section include, but are not limited to: a declaration that the interception or communication was unlawful; an order for payment of damages; an order, similar to or including, an injunction; and an order that the defendant pay the aggrieved person an amount not exceeding any income derived by the defendant as a result of the interception or communication: *Telecommunications (Interception and Access) Act 1979* (Cth) s 107A(7).

Surveillance device regulation by local councils

Question 13–2 Should local councils be empowered to regulate the installation and use of surveillance devices by private individuals?

13.58 A number of submissions have raised concerns regarding CCTV cameras, installed for security in homes and offices, but that may also record the activities of neighbours. Such uses of surveillance may be more appropriately regulated by local councils, rather than surveillance device laws.

13.59 By regulating surveillance devices at the local council level, it may be possible to resolve many disputes without recourse to the criminal law. A clear and transparent resolution process via local council would also potentially increase access to justice in circumstances where criminal penalties may be perceived as too severe.

13.60 Local governments are responsible for duties such as assessing and authorising development of houses, granting or disallowing various structural changes to property and protection of the environment. In New South Wales, for example, the *Environmental Planning and Assessment Act 1979* (NSW) and related planning instruments set out the types of development that require development consent from the local council. The installation of surveillance devices that overlook neighbouring properties could similarly require development consent.

13.61 Alternatively, the installation of surveillance devices could be included as a type of development that does not require development consent, provided certain conditions are met.[70]

13.62 Some councils already regulate surveillance devices. The City of Sydney Council, for example, has made determinations in the past on details such as the installation location and types of camera that may be used.[71] However, not all councils have such requirements.

13.63 Mechanisms for challenging local council decisions already exist in all states. For example, in NSW, review of a council's decision by the NSW Land and Environment Court is available under s 82A of the *Environmental Planning and Assessment Act 1979* (NSW). In Victoria, the Victorian Civil and Administrative Tribunal (VCAT) can hear appeals against decisions of planning and development applications made by local councils.[72]

---

70 The *State Environment Planning Policy (Exempt and Complying Development Codes) 2008* (NSW) (the Policy) sets out a range of developments which do not require council development consent, as long as certain conditions are met. For example, cls 2.3 and 2.4 of the Policy provide that development consent is not required for a aerial or antenna that at least 900mm away from a lot boundary and no higher than 1.8m above the highest point of the building's roof (if roof-mounted).

71 See, for example, *Szann v Council of City of Sydney* [2012] NSWLEC 1168 (21 June 2012).

72 *Planning and Environment Act 1987* (Vic) ss 77–86.

Civil penalties and interaction with the statutory cause of action

13.64 Some stakeholders suggested that a civil penalties regime should be considered to either complement or replace the criminal regime that currently exists under the surveillance device laws.[73] These stakeholders suggested that a civil penalties regime would be useful in light of the low levels of enforcement under the existing criminal regime. The VLRC has also recommended the introduction of a civil penalties regime in the *Surveillance Devices Act 1999* (Vic).[74]

13.65 There may be benefits in introducing a civil penalties regime into the surveillance device laws. For certain matters, a civil penalties process, potentially managed by a non-judicial regulator, could be cheaper, faster, and less burdensome than a criminal proceeding, both on the complainant and on the respondent. Additionally, criminal penalties may be unnecessarily severe for uses of surveillance devices that do not result in serious harm to the individual.

13.66 However, the ALRC has not proposed a civil penalties regime. The ALRC's proposal to allow courts to award compensation to victims of unlawful surveillance would achieve many of the objectives of a civil penalties regime, without the need to create new bodies to hear civil disputes about surveillance. Furthermore, the introduction of a statutory cause of action for serious invasion of privacy would provide another means of redress for unlawful surveillance. The introduction of a civil penalties regime for surveillance may result in overlap, excessive complexity and regulatory burden if a statutory cause of action were also introduced.

---

73 Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*.

74 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 19.

14. Harassment

Contents

Summary

14.1 The Terms of Reference for this Inquiry require the ALRC to make recommendations as to other legal remedies to redress serious invasions of privacy and innovative ways in which the law may reduce serious invasions of privacy.

14.2 Many serious invasions of privacy—perhaps some of the most serious—will also amount to harassment. Harassment involves a pattern of behaviour or course of conduct pursued by an individual designed to intimidate and distress another individual. The behaviour must be genuinely oppressive and vexatious and not amount to a mere irritation or annoyance. Laws that target harassment will often also serve to protect people's privacy.

14.3 The ALRC proposes that, if a new tort for serious invasion of privacy is not enacted, a Commonwealth harassment Act should be enacted that provides for a new tort of harassment. This Act would also consolidate and clarify existing criminal offences for harassment, including harassment using the internet.

14.4 This harassment legislation should be enacted by the Commonwealth. A federal Harassment Act will ensure consistent protection across Australia.

A Commonwealth harassment Act

Proposal 14–1 A Commonwealth harassment Act should be enacted to consolidate and clarify existing criminal offences for harassment and, if a new tort for serious invasion of privacy is not enacted, provide for a new statutory tort of harassment. Alternatively, the states and territories should adopt uniform harassment legislation.

14.5 This new Commonwealth harassment Act should consolidate existing federal, state and territory criminal offences for harassment. The offences should relate to harassment, irrespective of whether it occurred through online or telecommunications platforms, or through other physical or personal means.

14.6 If a new tort for serious invasions of privacy is not enacted, the ALRC proposes that this harassment Act should also include a civil action for harassment. This will help deter and redress some egregious types of invasion of privacy that are not currently the subject of effective legal protection.

Nexus between harassment and privacy

14.7 A serious invasion of privacy may often also amount to harassment. Harassment involves deliberate conduct. It may be done maliciously, to cause anxiety or distress or other harm, or it may be done for other purposes. Regardless of the intention, harassment will often cause anxiety or distress. Harassment also restricts the ability of an individual to live a free life.

14.8 The following is a list of examples of conduct that may in some cases amount to both a serious invasion of privacy as well as harassment where the conduct is repeated, unwanted and intended to distress and demean an individual:

- following or keeping under surveillance;
- eavesdropping and wiretapping;
- reading private letters and other private communication;[1]
- using surveillance devices to monitor, intimidate or distress someone, for example, through the use of cameras outside abortion clinics or aerial surveillance of private property using aircraft or unmanned aerial vehicles;[2]
- publishing personal data as a means of harassment, for example in the context of failed relationships or bullying or where incidents involving bullying are filmed and publicised as a means of further demeaning a victim;[3]
- pursuing a person in a sustained manner to track their private activities or to photograph them in private contexts, without their permission, including relentless pursuit by media or other parties; and
- communicating in a relentless and unwanted manner with an individual, such as through persistent telephone calls.[4]

---

1 Ruth Gavison, 'Privacy and the Limits of the Law' (1979) 89 *Yale Law Journal* 421, 429.

2 In *Howlett v Holding* [2006] EWHC 41 (QB) (25 January 2006) a UK court granted an injunction to restrain aerial surveillance under the *Protection from Harassment Act 1997* (UK). This case involved the defendant flying banners from private aircraft addressed to and referring to the plaintiff in derogatory terms, and dropping leaflets containing information about the plaintiff.

3 M Paterson, *Submission 60*.

4 Some of these are examples of conduct that has been the subject of claims under the *Protection from Harassment Act 1997* (UK).

Harassment Acts in other countries

14.9 Useful models for a Commonwealth Harassment Act include the UK's *Protection from Harassment Act 1997* and New Zealand's *Harassment Act 1997*.

14.10 The UK's *Protection from Harassment Act 1997* creates criminal offences when a person engages in a 'course of conduct' that amounts to harassment.[5] It is an offence for a person to pursue a course of conduct which amounts to harassment of another and which they know or ought to know amounts to harassment.[6] The Act defines harassment as having occurred if 'a reasonable person in possession of the same information would think the course of conduct amounted to harassment'.[7]

14.11 The Act provides for the award of civil remedies, including injunctions and damages to victims of harassment. The UK Act also creates the instrument of non-harassment orders. Where a person is convicted of the offence of harassment, a prosecutor may apply to the court to make a non-harassment order against the offender requiring them to refrain from 'such conduct in relation to the victim as specified in the order for such periods may be so specified'.[8]

14.12 New Zealand's *Harassment Act 1997* provides for harassment restraining orders and criminal penalties for harassment. The criminal offence of harassment applies where a person intends to cause fear to another person.[9] A person who is prosecuted for harassment can face up to two years imprisonment.[10] Plaintiffs can also apply to a court for a civil restraining order to prevent conduct amounting to harassment, breach of which will lead to penalties.[11] The New Zealand Act does not provide for compensation for victims. However, the common law has developed a tort of intrusion upon seclusion, which has been used to provide compensation for victims of harassment.[12]

14.13 A range of behaviours amounting to harassment have been successfully targeted through the UK and NZ harassment frameworks.[13]

14.14 Other comparable jurisdictions have enacted legislation to specifically target cyber-harms and so-called 'revenge pornography'.[14] New Zealand's government is currently considering legislation to tackle 'harmful digital communications' by way of

---

5 *Protection from Harassment Act 1997* (UK) ss 1, 2. The UK Supreme Court recently discussed the complexity in interpreting the Act: *Hayes (FC) v Willoughby* [2013] UKSC 17.
6 *Protection from Harassment Act 1997* (UK) s 1.
7 Ibid s 1(2).
8 Ibid s 11.
9 *Harassment Act 1997* (NZ) s 8.
10 Ibid.
11 Ibid s 9.
12 *C v Holland* [2012] 3 NZLR 672 (24 August 2012).
13 For example, cases of workplace harassment: *Majrowski v Guy's and St Thomas' NHS Trust* [2006] UKHL 34; aerial surveillance over private property: *Howlett v Holding* [2006] EWHC 41 (QB); restraining media and paparazzi from following individuals: *Thomas v News Group Newspapers Ltd* [2002] EMLR 78.
14 Eg, New Jersey legislation criminalises the reproduction or disclosure of images of sexual contact without consent: *NJ Rev Stat* § 2C:14-9 (2013).

the Harmful Digital Communications Bill 2013. If enacted, the legislation would prohibit an individual from sending a message to another person—for example by text, online publication or email—where the conduct of that message is grossly indecent, obscene, menacing or knowingly false, and where the sender intends the message to cause emotional distress to the recipient.[15] This offence would be punishable by up to three months imprisonment or a NZ$2,000 fine.

14.15 Nova Scotia's *Cyber-Safety Act 2013* creates a tort of cyber-bullying so that 'a person who subjects another person to cyber-bullying commits a tort against that person'.[16] Cyber-bullying is defined in this Act as using 'electronic communication through the use of technology, including … social networks, text messaging, instant messaging, websites and electronic mail … typically repeated or with continuing effect, that is intended or ought reasonably to be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation'.[17] In an action for cyber-bullying, a court may award damages including general, special, aggravated and punitive damages.[18] A court may also issue an injunction[19] or make an order that the court considers 'just and reasonable in the circumstances'.[20]

Civil remedies

14.16 The courts in Australia have not recognised a common law cause of action for harassment. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, Gummow and Hayne JJ referred to 'what may be a developing tort of harassment',[21] citing the work of Professor Stephen Todd from New Zealand.[22] New Zealand has now enacted the *Harassment Act 1997* (NZ) and the courts have recognised a tort of intrusion into seclusion.[23]

14.17 In *Grosse v Purvis*[24] a Queensland District Court judge recognised an actionable right to privacy, after a finding that the defendant had persistently and intentionally stalked and harassed the plaintiff for six years. Because of his conclusion on the actionable right to privacy, there was no need to decide whether a tort of harassment should be recognised.

---

15 Harmful Digital Communications Bill 2013 (NZ) cl 19.
16 *Cyber-Safety Act*, SNS 2013, c 2 2013 s 3(b).
17 *Cyber-Safety Act 2013* (SNS) s 3(b).
18 Ibid s 22(1)(a).
19 Ibid s 22(1)(b).
20 Ibid s 22(1)(c).
21 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [123].
22 Stephen Todd, 'Protection of Privacy' in Nicholas Mullany (ed), *Torts in the Nineties* (LBC Information Services, 6th ed, 1997).
23 *C v Holland* [2012] 3 NZLR 672 (24 August 2012).
24 *Grosse v Purvis* [2003] QDC 151 (16 June 2003); Des A Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 352. Doubt has been expressed about the correctness of *Grosse v Purvis*: see Ch 3. The case was settled before the defendant's appeal was heard.

14.18 Many instances of harassment will involve a serious invasion of privacy and yet not give rise to an existing tort. As discussed in Chapter 3, this is a significant gap in the protection of privacy by the common law.[25]

14.19 For example, the tort of trespass to land can be used only where there has been an unlawful intrusion *onto* property.[26] Surveillance or harassment from *outside* the property would not come within the tort. Further, the harassment may occur on property where the victim is not the occupier with the required title to sue for trespass.[27]

14.20 The harassment may not involve any physical contact amounting to the tort of battery and may not involve a *threat* of physical contact which is necessary for a tort action in assault.[28]

14.21 The tort of nuisance requires an interference with the lawful occupier's use and enjoyment of land.[29] Nuisance has been useful in limited cases such as where a CCTV camera is erected at a neighbour's backyard, prohibiting their use and enjoyment of the garden.[30] However, again, a person's right to sue is limited.[31]

14.22 The tort of wilful infliction of nervous shock[32] is an inadequate remedy for many instances of harassment as a claimant must prove actual physical or psychiatric injury. Harassment, however, will often result only in emotional distress.

14.23 A new tort for harassment would provide for a targeted avenue for civil redress where the conduct is not redressed by existing torts.

Criminal offences

14.24 State, territory and federal laws provide a number of criminal offences relating to different forms of harassment across. There would be advantages in clarifying, consolidating and making uniform the range of criminal offences for harassment across Australia.

14.25 State and territory criminal laws criminalise harassment and stalking conducted through online or other forms of electronic communication. However, these offences vary considerably depending on the jurisdiction. For instance, legislation in Queensland criminalises harassment through all forms of electronic communication in the offence of stalking by 'otherwise contacting the victim'.[33] In Victoria, the definition of stalking extends to a course of conduct committed via 'electronic

25 See Barbara McDonald, 'Tort's Role in Protecting Privacy: Current and Future Directions' in James Edelman, James Goudkamp and Degeling (eds), *Torts in Commercial Law* (Thomson Reuters, 2011).
26 *Plenty v Dillon* (1991) 171 CLR 635.
27 *Kaye v Robertson* [1991] FSR 62.
28 RP Balkin and JLR Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [3.16].
29 Ibid [14.1].
30 *Raciti v Hughes* (1995) 7 BPR 14837.
31 *Hunter and Others v Canary Wharf Ltd; Hunter and Others v London Docklands Corporation* [1997] UKHL 14.
32 *Wilkinson v Downton* (1897) 2 QB 57; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.
33 *Criminal Code Act 1899* (Qld) s 395A(7)(b).

communications'.[34] The National Children's and Youth Law Centre supported the need to 'address the gaps' in the current legal frameworks for cyber-bullying and harassment.[35]

14.26 The Commonwealth *Criminal Code*[36] provides for an offence of 'using a carriage service to menace, harass or cause offence'[37] and 'using a carriage service to make a threat'.[38] These would capture conduct amounting to harassment, for example, via the internet, including social media, and telephone.[39]

14.27 There are also laws to protect victims of family violence from harassment, including harassment via electronic communications. For example, stalking is included in the definition of 'family violence' in the *Family Law Act 1975* (Cth).[40]

14.28 The Australian Government Department of Communications is currently conducting a review into online safety for children.[41] The Department has been asked to consider simplifying the meaning and application of s 474.17 of the *Criminal Code*. The Department's Discussion Paper suggested that 'the existing offence is worded in a way that people, particularly minors, would not understand'.[42] The Department has outlined three options for reform. First, to retain the existing provision and implement education to raise awareness of its potential application. Secondly, to create a cyber-bullying offence with a civil penalty regime for minors, and thirdly, to create a take-down system and accompanying infringement notice scheme to regulate complaints about online content.

A Commonwealth Act or uniform legislation

14.29 There are a number of suitable constitutional heads of power which may enable the Commonwealth to enact legislation on harassment.[43] A new Commonwealth Harassment Act may be supported by the external affairs power.[44] It may be argued that harassment constitutes 'an arbitrary or unlawful interference with ... privacy,

---

34 *Crimes Act 1958* (Vic) s 21A(2)(b).

35 National Children and Youth Law Centre, *Submission 61*.

36 This point was made in: Department of Communications Australian Government, 'Enhancing Online Safety for Children: Public Consultation on Key Election Commitments' (January 2014).

37 *Criminal Code* (Cth) s 474.17.

38 Ibid s 474.15.

39 At the Bullying, Young People and the Law Symposium hosted by the Alannah and Madeline Foundation in Sydney from July 18-19 2013, delegates recommended that Australian governments introduce a specific, and readily understandable, criminal offence of bullying, including cyber-bullying, involving a comparatively minor penalty to supplement existing laws which are designed to deal with more serious forms of conduct.

40 *Family Law Act 1975* (Cth) s 4AB(2)(c).

41 The Department of Communications released a public discussion paper on 22 January 2014 and was awaiting submissions to that discussion paper by 7 March 2014. Australian Government 2014, 'Enhancing Online Safety for Children: Public Consultation on Key Election Commitments', discussion paper, Department of Communications. The Government has founded an Online Safety Consultative Working Group to provide advice to government on online safety issues.

42 Ibid.

43 See also the discussion of constitutional issues in Ch 4.

44 *Australian Constitution* s 51(xxix).

family, home or correspondence',[45] or some other interference with fundamental liberties protected by the ICCPR.

14.30 Alternatively, a new Act may be supported by s 51(v) of the *Australian Constitution*. A court would likely hold that this head of power supports a law regulating harassment effected by postal, telegraphic and telephonic services, as well as online services. However, the new Act is intended to cover both online and offline forms of harassment. It is unlikely that the latter category would be supported by s 51(v).

14.31 By way of comparison, the sexual harassment provisions in the *Sex Discrimination Act 1984* (Cth)[46] are supported by numerous heads of power including the external affairs power in relation to the *Convention on the Elimination of all Forms of Violence against Women*.[47]

14.32 If the Commonwealth does not have the power to enact harassment legislation, covering both so-called 'online' and 'offline' harassment, the ALRC proposes that the states and territories adopt uniform harassment legislation. National consistency in privacy law is important as inconsistency can lead to fragmentation, poor protection for all individuals in Australia and can also burden business.[48]

14.33 The ALRC welcomes stakeholder submissions on these constitutional issues, in addition to comments on the proposal overall.

---

45 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17(1).

46 *Sex Discrimination Act 1984* (Cth).

47 *Convention on the Elimination of All Forms of Discrimination Against Women*, opened for signature 18 December 1980, 1249 UNTS (entered into force 3 September 1981).

48 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) 3.13.

15. New Regulatory Mechanisms

Contents

Summary

15.1 This chapter sets out proposals and questions about new regulatory mechanisms to reduce and redress serious invasions of privacy. The new regulatory powers proposed in this chapter are not intended to be an alternative to the new tort. The ALRC considers that these powers could operate alongside the new tort.

15.2 Two regulatory bodies are considered. The first is the Australian Communications and Media Authority (ACMA) which has powers relating to the broadcast media under the *Broadcasting Services Act 1992* (Cth). The second is the Office of the Australian Information Commissioner (OAIC) which has powers relating to information privacy under the *Privacy Act 1988* (Cth).

15.3 In this chapter, the ALRC first proposes that the ACMA be empowered to make a determination that a complainant should be compensated where a broadcaster's conduct amounts to a serious invasion of the complainant's privacy in breach of a broadcasting code of practice. The proposed new power of the ACMA would be similar to existing powers of the OAIC.

15.4 Secondly, the ALRC proposes the introduction of a new Australian Privacy Principle (APP) which would require APP entities to take reasonable steps to delete personal information about an individual on request. The ALRC has also asked a

question about a possible take-down system that would empower a regulator to require an organisation to remove information about an individual from a website or online service, where the publication of that information is a serious invasion of privacy. The regulator would be required to have regard to freedom of expression and other public interests. This may be a fast, low-cost mechanism to limit the risk, extent, and harm of a serious invasion of privacy.

15.5 Thirdly, the ALRC proposes that the statutory functions of the Australian Information Commissioner[1] be amended to include acting as amicus curiae and intervening in appropriate court proceedings, with leave of the court.

15.6 In this chapter, the ALRC also discusses the small business exemption to the *Privacy Act* and an extended complaints process for the OAIC.

Expanding the ACMA's powers

Proposal 15–1 The ACMA should be empowered, where there has been a privacy complaint under a broadcasting code of practice and where the ACMA determines that a broadcaster's act or conduct is a serious invasion of the complainant's privacy, to make a declaration that the complainant is entitled to a specified amount of compensation. The ACMA should, in making such a determination, have regard to freedom of expression and the public interest.

Existing powers of the ACMA relating to codes of practice

15.7 The ACMA has regulatory powers over broadcasting (including radio and television) and telecommunications. These powers are granted primarily under the *Australian Communication and Media Authority Act 2005* (Cth), the *Broadcasting Services Act 1992* (Cth), the *Telecommunications Act 1997* (Cth). Regulatory powers in relation to specific privacy issues are also granted to the ACMA under the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2009* (Cth).

15.8 The ACMA's powers are primarily exercised by promoting self-regulation (in which industry members regulate themselves under industry guidelines, codes or standards) and co-regulation (in which industry members develop guidelines, codes or standards that are enforceable under legislation).

15.9 Privacy provisions with public interest exceptions exist in a range of broadcasting industry codes of practice. The privacy provisions of the codes relating to broadcasters are limited to broadcasts of news and current affairs programs.[2]

---

1 The *Privacy Act 1988* (Cth) currently confers a number of functions on the Australian Information Commissioner.

2 Commercial Television Industry Code of Practice 2010 cl 4.3.5; Commercial Radio Codes of Practice and Guidelines 2011 cl 2.1(d); ABC Code of Practice 2011 cl 6.1; SBS Codes of Practice 2014 cl 1.9.

15.10 If a code is breached, the ACMA may: determine an industry standard;[3] make compliance with the code a condition of the broadcaster's license;[4] or accept an enforceable undertaking from the broadcaster that the broadcaster will comply with the code.[5] Further consequences—including civil penalties, criminal penalties, and suspension or cancellation of a broadcaster's license—exist for a breach of a standard,[6] a license condition[7] or an enforceable undertaking.[8]

15.11 Distinct powers exist if a complaint is made against the ABC or SBS. In these cases, the ACMA may recommend that the broadcaster take action to comply with the relevant code, or that the broadcaster take other action including publishing an apology or retraction.[9]

15.12 The ACMA does not have the power to determine that compensation be paid to an individual whose privacy has been seriously invaded by a broadcaster.

An extension of the ACMA's powers

15.13 The ALRC's proposal would grant a new power allowing the ACMA to make a declaration that a complainant should be compensated for any loss or damage suffered from a serious invasion of privacy by a broadcaster. This would provide the ACMA with a power similar to that held by the OAIC under the *Privacy Act 1988* (Cth).[10] However, the relevant provisions of the *Privacy Act* do not apply to a media organisation acting in a journalistic capacity if the organisation has publicly committed to observing privacy standards.[11]

15.14 Granting this power to the ACMA would help to address the limitation of the *Broadcasting Services Act* that an individual is not entitled to compensation or other forms of personal redress when their privacy is invaded in breach of a broadcasting code of conduct. Granting this power would also provide consistency between the powers of the OAIC and the powers of the ACMA in respect of privacy.

15.15 Under this proposal, the ACMA would be empowered to make a declaration for compensation only in cases where an invasion of privacy was serious. This condition would not be met by all invasions of privacy under relevant codes of practice.

15.16 It is important to note that any determination made by the OAIC under s 52(1A) of the *Privacy Act* must be enforced in the Federal Court or Federal Circuit Court.[12] A

---

3 *Broadcasting Services Act 1992* (Cth) s 125.
4 Ibid s 44.
5 Ibid s 205W.
6 Ibid pt 9B div 5.
7 Ibid pt 10 div 3.
8 Ibid pt 14D.
9 Ibid ss 150–152.
10 Under s 52(1A)(d) of the *Privacy Act*, the Australian Information Commissioner, in response to a complaint, may make a determination including a declaration that the respondent pay an amount of compensation to the complainant.
11 *Privacy Act 1988* (Cth) s 7B(4).
12 Ibid s 55A.

similar procedure would be required to enforce a declaration made by the ACMA under the new power proposed by the ALRC.

15.17 Strengthening the ACMA's powers in respect of serious invasions of privacy would help deter serious invasions of privacy by broadcasters and provide individuals with an alternative to costly litigation.

15.18 Any expansion of the ACMA's powers would need to take into account the self-regulatory nature of the *Broadcasting Services Act*. One of the objects of the Act is to '[enable] public interest considerations to be addressed in a way that does not impose unnecessary financial and administrative burdens on providers of broadcasting services'.[13] The ACMA similarly noted in its submission that:

> The relevant legislative framework therefore requires the ACMA to provide industry with the opportunity to develop co and self-regulatory solutions, before other forms of intervention are considered.[14]

15.19 The power to be exercised under this proposal would only be engaged where there has been a failure to comply with a self-regulatory code. The proposed power would be arguably less burdensome on media organisations than alternative mechanisms for increasing privacy protections, such as removing the media exemption to the *Privacy Act 1988*.

15.20 Some media organisations submitted that any additional privacy protections would impose an excessive regulatory burden on the media and may have a chilling effect on responsible journalism.[15] While the ALRC acknowledges the range of laws affecting media organisations, it should be noted that many of these laws protect privacy only in an incidental and limited way, and that there are significant gaps and deficiencies in the protection of privacy.[16] It should also be reiterated that the proposed extension to the ACMA's powers would only apply to those complaints which are serious and for which there is no overriding public interest justification.

15.21 There is some evidence that privacy complaints against the media are relatively rare. The ACMA's 2012–13 Annual Report showed that, while there were a total of 2178 enquiries and written complaints about commercial, national and community television broadcasters, there were only two breach findings relating to privacy by commercial television broadcasters, and only three non-breach findings.[17] Rather than providing evidence that no further privacy protections are needed, the ALRC suggests

---

13 *Broadcasting Services Act 1992* (Cth) s 4(2).

14 Australian Communications and Media Authority, *Submission 52*.

15 SBS, *Submission 59*; Free TV, *Submission 55*; The Newspaper Works, *Submission 50*; Australian Subscription Television and Radio Association, *Submission 47*; ABC, *Submission 46*. The submission from Free TV included a list of existing laws affecting media organisations, including laws relating to: trespass; nuisance; confidential information; defamation; malicious falsehood; contempt; data protection (however, as noted above, the *Privacy Act 1988* (Cth) contains an exemption for media organisations); criminal trespass laws; restrictions on reporting matters affecting or involving children, adoption, coronial inquiries, sexual offences, jurors, and prisoners; court orders to make orders restricting reporting of court proceedings; anti-discrimination; restrictions on reporting certain types of activity under, for example, the *Australian Security Intelligence Organisation Act 1979* (Cth); family law; and surveillance devices.

16 See Ch 3 for further analysis of existing laws.

17 'Annual Report 2012-13' (Australian Communications and Media Authority) app 6.

that the ACMA's figures indicate that the additional power proposed may be rarely used. However, the proposed power would provide a means of redress and alternative dispute resolution to affected individuals without the high cost for both parties of litigation.

A new privacy principle for deletion of personal information

Proposal 15–2 A new Australian Privacy Principle should be inserted into the *Privacy Act 1988* (Cth) that would:

(a) require an APP entity to provide a simple mechanism for an individual to request destruction or de-identification of personal information that was provided to the entity by the individual; and

(b) require an APP entity to take reasonable steps in a reasonable time, to comply with such a request, subject to suitable exceptions, or provide the individual with reasons for its non-compliance.

Question 15–1 Should the new APP proposed in Proposal 15–2 also require an APP entity to take steps with regard to third parties with which it has shared the personal information? If so, what steps should be taken?

The importance of deletion

15.22 Several submissions to the Issues Paper noted that the harm caused by a serious invasion of privacy in the digital era will often increase the longer private information remains accessible.[18] Ensuring that individuals have a means to rapidly remove such information is one way to reduce the availability of private information. This proposal, if enacted, would provide a mechanism to assist individuals in having certain personal information destroyed or de-identified. The risk of that information being misused or disclosed in the future would thereby be reduced.

15.23 This proposal would not provide a mechanism to allow individuals to request the deletion of private information posted about them by other individuals or organisations. In this respect, the proposal is significantly different from the 'Right to be Forgotten', which has been considered in the European Union[19] and which was referred to in the Issues Paper.[20]

18 National Children and Youth Law Centre, *Submission 61*; Google, *Submission 54*; Australian Privacy Foundation, *Submission 39*; B Arnold, *Submission 28*.

19 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

20 Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era' (Issues Paper 43, 2013) 50.

Limits of the proposed privacy principle

15.24 The proposed privacy principle includes two key requirements. First, an APP entity (as defined in the *Privacy Act 1988* (Cth)) would be required to provide a mechanism for individuals to request the deletion or de-identification of personal information held by that entity. Such a mechanism is already provided by some online services, allowing individuals to delete information that they have previously added to the service.[21]

15.25 The second element of the proposal would require an APP entity that receives such a request to take reasonable steps to destroy or de-identify the relevant personal information in a reasonable time. Such a requirement would be subject to certain exceptions including, for example, where the information is required by law to be retained.[22] An organisation which did not destroy or de-identify the information would be required to provide the requesting individual with the reason for its decision.

The context of the *Privacy Act*

15.26 The proposed privacy principle would be contained within the *Privacy Act 1988* (Cth), along with the thirteen existing Australian Privacy Principles (APPs). The existing APPs include similar, but weaker, requirements. First, an APP entity must take reasonable steps to correct personal information held about an individual at the individual's request.[23] Second, an APP entity must destroy or de-identify personal information that is no longer required for a specific purpose under the APPs.[24] The proposed privacy principle would complement these existing APPs. First, an individual would be empowered not only to request correction of personal information but also to request its deletion. Second, deletion would be required not only when the personal information is no longer useful but also when the individual requests its deletion.

15.27 As an APP, the proposed principle would engage the existing complaints and enforcement mechanisms of the Office of the Australian Information Commissioner. In particular:

- an APP entity's failure to comply with the principle would constitute an interference with the privacy of an individual under the *Privacy Act*;[25]
- an affected individual could therefore make a complaint about the failure to the OAIC;[26] and
- a serious or repeated failure to comply with the principle would constitute a breach of a civil penalty provision, possibly resulting in pecuniary penalties.[27]

---

21 Facebook, *Submission 65*.
22 For example, limits are placed on the destruction or alteration of Commonwealth records under the *Archives Act 1983* (Cth) s 24.
23 *Privacy Act 1988* (Cth) sch 1 cl 13.
24 Ibid sch 1 cl 11.
25 Ibid s 13(1).
26 Ibid ss 36, 40, 52.
27 Ibid s 13G.

Extending the deletion requirement for data-sharers

15.28 The ALRC has asked whether the proposed privacy principle should also require an APP entity to take additional steps where a deletion request is made and the relevant information has been shared with third parties. The ALRC has also asked what additional steps should be required in such cases. Some possible examples of additional steps include:

- requiring the APP entity who receives the request to provide the requesting individual with a list of third parties who have received the information; and
- requiring the APP entity who receives the request to notify any third parties with which it has shared the information that the request has been made.

15.29 The utility of any such additional requirements would likely depend on the extent to which personal information collected by one APP entity is shared with other APP entities. However, the ALRC also acknowledges that, depending on the steps required, this extension of the proposed privacy principle may introduce additional burdens on APP entities.

Regulator take-down orders

Question 15–2 Should a regulator be empowered to order an organisation to remove private information about an individual, whether provided by that individual or a third party, from a website or online service controlled by that organisation where:

(a) the individual makes a request to the regulator to exercise its power;

(b) the individual has made a request to the organisation and the request has been rejected or has not been responded to within a reasonable time; and

(c) the regulator considers that the posting of the information constitutes a serious invasion of privacy, having regard to freedom of expression and other public interests?

15.30 The new Australian Privacy Principal in Proposal 15–2 does not include any right for an individual to have personal information deleted or de-identified when that information is provided by a third party. There may, however, be merit in introducing a take-down mechanism by which an individual could apply to have such information removed from websites and other online services. As noted above, the rapid removal of privacy information from public websites may help prevent an invasion of privacy. Although some online service providers may offer a system for complaining about a serious invasion of privacy, others may not.[28]

---

28 The ALRC previous considered a take-down system in ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [11.21]–[11.23]. However, the possibility of a take-down mechanism continues to be discussed, and so it has been raised again in this Discussion Paper.

15.31 A regulator take-down system may provide a mechanism for limiting the impact or serious invasions of privacy. However, there is also a risk that such a system may have an undesirably chilling effect on online freedom of expression. The ALRC has therefore sought comment on the desirability of a take-down system, but has not proposed a take-down system at this stage. Comments are sought on:

- whether any such take-down system is desirable;
- which regulator or regulators should be empowered to issue take-down orders;
- the circumstances in which a take-down order should be issued; and
- any ways in which negative impacts on free expression could be minimised.

15.32 If the statutory cause of action for serious invasion of privacy is enacted, an individual who has suffered a serious invasion of privacy may apply to a court for an injunction requiring the removal of private information.

15.33 However, applying for an injunction may be expensive and time-consuming for the affected individual. A take-down system operated by a regulator would potentially be a cheaper and quicker alternative. It may also be a more accessible alternative where the affected individual is a young person. The OAIC and the ACMA may be well-suited to exercising a power to order take-downs.

15.34 The ALRC has suggested a model whereby a take-down order could be issued if three conditions are met. First, the regulator must receive a complaint from an individual. This would ensure that the regulator could not order a take-down of its own motion. Second, the individual must have attempted, without success, to have the material removed by the organisation which controls the website or online service. This would ensure that individuals had attempted to deal with the matter themselves before engaging the regulator. Third, the regulator must consider that the posting of the information constitutes a serious invasion of privacy, having regard to freedom of expression and other public interests. This would ensure that take-downs would only be ordered where an invasion was serious and where there was no countervailing interest in freedom of expression or public interest.

15.35 As noted above, the Department of Communications is currently engaged in an inquiry into Online Safety for Children. As part of that inquiry, the Department has proposed a Commissioner with the power to issue a notice requiring the removal of material that is likely to harm a child. Such a notice could, under the Department's proposal, be directed to either the internet intermediary[29] or the individual who posted the material.

29 See Ch 10 on the meaning of 'internet intermediaries'.

Amicus curiae and intervener roles for the Australian Information Commissioner

Proposal 15–3 The *Privacy Act 1988* (Cth) should be amended to confer the following additional functions on the Australian Information Commissioner in relation to court proceedings relating to interferences with the privacy of an individual:

(a) assisting the court as amicus curiae, where the Commissioner considers it appropriate, and with the leave of the court; and

(b) intervening in court proceedings, where the Commissioner considers it appropriate, and with the leave of the court.

15.36 The ALRC has proposed that the Australian Information Commissioner be given new functions to act as amicus curiae or to intervene in legal proceedings relating to the information privacy. These functions would be additional to a range of existing functions conferred on the Commissioner under ss 27–29 of the *Privacy Act 1988* (Cth), including:

- specific functions under the *Privacy Act* (such as responding to complaints from individuals);
- guidance related functions (preparing guidance about and promoting understanding of the requirements of the *Privacy Act*);
- monitoring related functions (ensuring that APP entities are meeting the requirements of the *Privacy Act* and ensuring that any privacy impacts of new laws, practices or proposals are minimised); and
- advice related functions (providing advice about the operation of and compliance with the *Privacy Act*, and any need for legislative action).

15.37 These additional functions would be similar to functions conferred on other administrative bodies, such as the ACCC, ASIC and the Human Rights Commission.

The role of an amicus curiae

15.38 The role of an amicus curiae ('friend of the court') is to assist the court 'by drawing attention to some aspect of the case which might otherwise be overlooked.'[30] An amicus curiae may 'offer the Court a submission on law or relevant fact which will assist the Court in a way in which the Court would not otherwise have been assisted'.[31] This role does not extend to introducing evidence to the court, although an amicus may

30 *Bropho v Tickner* (1993) 40 FCR 165, 172 (Wilcox J). On the role of an amicus curiae generally, see Australian Law Reform Commission, *Beyond the Door-Keeper: Standing to Sue for Public Remedies*, Report 78 (1996) ch 6.

31 *Levy v Victoria* (1997) 189 CLR 579, 604 (Brennan CJ).

be permitted to lead non-controversial evidence in order to 'complete the evidentiary mosaic'.[32] An amicus curiae is not a party to the proceedings and is not bound by the outcome of the proceedings. In *Re United States Tobacco Company*, Einfeld J noted the value of amici curiae, particularly as subjects of increasing complexity are brought before the courts:

> The variegated complexity of modern life and technology, increasing materialism and the possible risks to the public of otherwise lauded scientific advances, have brought consequent significant legal challenges. These have been amplified not minimally by the burgeoning of statutory law expressing vague general principles and requiring the exercise of broad undefined judicial discretions. For the just resolution of these issues, the resultant mix beckons, if not requires, whatever assistance and expertise the Courts can reasonably muster.[33]

15.39 An example of legislation conferring an amicus curiae function onto an administrative body can be found in s 46PV of the *Australian Human Rights Commission Act 1986* (Cth). This section allows individual Commissioners ('special-purpose Commissioners') within the Commission to act as amici curiae, with the court's leave:

> (1) A special-purpose Commissioner has the function of assisting the Federal Court and the Federal Circuit Court, as amicus curiae, in the following proceedings under this Division:
>
> (a) proceedings in which the special-purpose Commissioner thinks that the orders sought, or likely to be sought, may affect to a significant extent the human rights of persons who are not parties to the proceedings;
>
> (b) proceedings that, in the opinion of the special-purpose Commissioner, have significant implications for the administration of the relevant Act or Acts;
>
> (c) proceedings that involve special circumstances that satisfy the special-purpose Commissioner that it would be in the public interest for the special-purpose Commissioner to assist the court concerned as amicus curiae.

15.40 Importantly, an amicus curiae does not have a legal interest in the outcome of proceedings. A person with a legal interest in proceedings may instead, with the leave of the court, intervene in the proceedings.

The role of an intervener

15.41 The role of amicus curiae can be distinguished from the role of an intervener. While the role of an amicus curiae is to assist the court, the role of an intervener is to represent the intervener's own legal interests in proceedings.

15.42 An intervener's legal interests may be affected in a number of ways. First, the intervener's interests may be directly affected by the court's decision. For example, a decision about the property interests of the parties to proceedings might also affect the

---

32 *Bropho v Tickner* (1993) 40 FCR 165, 172 (Wilcox J).

33 *Re United States Tobacco Company v the Minister of Consumer Affairs and the Trade Practices Commission* [1988] FCA 241 (14 July 1988) [68] (Einfeld J).

property interests of the intervener. Second, the intervener's interests may be less directly affected. For example, the court's decision might have an effect on the future interpretation of laws affecting the intervener.[34] Under the ALRC's proposal, a court might, for example, give leave to the Australian Information Commissioner to intervene in a case that would have future repercussions for the work of the OAIC.

15.43 Functions to intervene are conferred upon a number of administrative bodies. For example, s 11(1)(o) of the *Australian Human Rights Commission Act 1986* (Cth) confers an intervention function on the Australian Human Rights Commission:

> where the [Australian Human Rights Commission] considers it appropriate to do so, with the leave of the court hearing the proceedings and subject to any conditions imposed by the court, to intervene in proceedings that involve human rights issues[.][35]

15.44 The Australian Competition and Consumer Commission (ACCC) has an intervention function in relation to proceedings under the *Competition and Consumer Act 2010* (Cth).[36] The Australian Securities and Investments Commission has an intervention function in relation to proceedings about consumer protection in financial services.[37]

Other regulatory reforms

Small businesses

15.45 The APPs under the *Privacy Act 1988* (Cth) regulate the handling of personal information by APP entities, ie government agencies and organisations.[38] Notably, small businesses with an annual turnover of less than $3 million[39] are exempt from the definition of 'organisation' and thus from the ambit of the APPs unless, for instance:

- the small business trades in personal information;
- the small business handles health information; or
- the small business operator notifies the OAIC in writing of its desire to be treated as an organisation.[40]

15.46 In its 2008 report *For Your Information*, the ALRC recommended that the small business exemption be removed from the *Privacy Act*. Several stakeholders, in submissions to the ALRC's current Inquiry, noted that the exemption remains in the *Privacy Act*, and that the removal of the exemption would have benefits for privacy.[41]

---

34 *Levy v Victoria* (1997) 189 CLR 579, 601–602 (Brennan CJ).

35 The Australian Human Rights Commission also has intervention functions, see for example, *Australian Human Rights Commission Act 1986* (Cth) s 31(j); *Sex Discrimination Act 1984* (Cth) s 48(1)(gb); *Racial Discrimination Act 1975* (Cth) s 20(e); *Disability Discrimination Act 1992* (Cth) s 67(1)(1); *Age Discrimination Ac 2004* (Cth) s 53(1)(g).

36 *Competition and Consumer Act 2010* (Cth) s 87CA.

37 *Australian Securities and Investments Commission Act 2001* (Cth) s 12GO.

38 *Privacy Act 1988* (Cth) s 6(1) (definition of 'APP entity').

39 Ibid ss 6C, 6D.

40 Ibid ss 6D, 6E, 6EA.

41 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 39–1.

15.47 Ensuring that small businesses handle personal information in an appropriate way may be particularly important in the digital era. A small business in the digital era can readily collect personal information through, for example, software on mobile phones or websites.[42] Removing the small business exemption may therefore provide for better information privacy protections in the digital era.

15.48 The ALRC acknowledges, however, that removing the small business exemption may have compliance costs for small businesses. The ALRC considers that the small business exemption should be given further consideration, particularly given the growth of digital communications and the digital economy since the 2008 recommendation. The Productivity Commission, for instance, may be well-placed to investigate the likely impacts on small businesses if the small business exemption were removed. Such an investigation could give detailed consideration to the application of limited data protection models to small businesses in other jurisdictions[43] as well as other options for improving the protection of personal information held by small business.[44]

An extended complaints process for the OAIC

15.49 In its submission to Issues Paper 43, the Office of the Australian Information Commissioner outlined a proposal for a new 'complaints model'. The OAIC suggested that this model could provide an alternative to the statutory cause of action for serious invasions of privacy. A core element of the OAIC's proposal would be a new power granted to the Australian Information Commissioner to receive complaints from individuals about intrusions into seclusion. This new power would extend the existing powers of the Commissioner to hear complaints about breaches of the APPs.

15.50 An intrusion into seclusion would, under the OAIC's proposal, constitute an 'interference with the privacy of an individual'.[45] This would allow the individual to bring a complaint to the Commissioner,[46] or for the Commissioner to undertake an own motion investigation.[47] In the event that the Commissioner determined that an intrusion into seclusion had occurred, the existing powers of the Commissioner would allow for

---

42 'Mobile Apps' (Occasional paper 1, Australian Communications and Media Authority, May 2013); 'The Cloud—services, Computing and Digital Data' (Occasional paper 3, Australian Communications and Media Authority, June 2013); 'Mobile Privacy: A Better Practice Guide for Mobile App Developers' (Office of the Australian Information Commissioner, September 2013).

43 *Data Protection Act 1998* (UK).

44 For example, the small business exemption could be limited so that small businesses handling sensitive information would not be exempt. Sensitive information includes personal information about an individual's racial or ethnic origin, political opinions, membership of political associations, religious beliefs or affiliations, philosophical beliefs, professional or union membership, sexual orientation or practices or criminal record, as well as health information, genetic information, and certain types of biometric information: *Privacy Act 1988* (Cth) s 6(1) (definition of 'sensitive information').

45 Ibid s 6(1) (definition of 'interference with the privacy of an individual').

46 Ibid s 36.

47 Ibid s 40.

a range of declarations to be made.[48] A determination of the Commissioner would then be enforceable through the Federal Court or Federal Circuit Court.[49]

15.51 In the event that the intrusion into seclusion was serious or repeated, the intrusion would be a contravention of a civil penalty provision. The Commissioner would then be empowered to apply to the Federal Court or Federal Circuit Court for an order that the respondent pay a civil penalty.[50]

15.52 The ALRC acknowledges that the OAIC's proposed complaints model may offer several advantages over other methods of dealing with privacy disputes, in particular through litigation. Most significantly, the complaints model may be cheaper and faster than litigation, and may be less taxing on parties to a dispute. The complaints model would also take advantage of the OAIC's existing powers and expertise in handling complaints about information privacy.

15.53 However, the OAIC's proposed complaints model would face several challenges. First, as noted by the OAIC in its submission, the model would require substantial additional OAIC resourcing, particularly if the complaints process were to be readily available across the country. Second, also as noted by the OAIC, the respondents to complaints under the existing *Privacy Act* are typically government agencies and large businesses. Although it may be possible to extend the *Privacy Act* to include complaints against individuals more generally, such an extension may have significant consequences which would need detailed consideration. Third, the *Privacy Act* contains a range of exemptions, such as the small business exemption noted above. While these exemptions remain in place, a complaints process based on the *Privacy Act* would have significant limitations.

15.54 For these reasons, the ALRC has not proposed extending the *Privacy Act* or the powers of the Australian Information Commissioner in the way proposed in the OAIC submission. However, the ALRC notes that further consideration of the complaints model may be appropriate in the future.

---

48 These declarations could include: that the complainant is entitled to an amount of compensation; that the respondent should perform specific actions to ensure that the intrusion does not occur again; or that the respondent should perform specific actions to redress any loss or damage suffered by the complainant: Ibid s 52.

49 Ibid s 55A.

50 Ibid ss 13G, 80U, 80W, 80X.