Australian Government
Australian Law Reform Commission

Serious Invasions of Privacy in the Digital Era

FINAL REPORT

ALRC Report 123

June 2014

This Final Report reflects the law as at 30 June 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: 978-0-9924069-1-2

Commission Reference: ALRC Final Report 123, 2014

© Commonwealth of Australia 2014

This work is copyright. You may download, display, print and reproduce this material in whole or part, subject to acknowledgement of the source, for your personal, non-commercial use or use within your organisation. Requests for further authorisation should be directed to the ALRC.

Printed by Ligare Pty Ltd

Australian Government

Australian Law Reform Commission

The Hon George Brandis QC MP
Attorney-General of Australia
Parliament House
Canberra ACT 2600

30 June 2014

Dear Attorney-General

ALRC Terms of Reference—Serious Invasions of Privacy in the Digital Era

On 12 June 2013, the Australian Law Reform Commission received Terms of Reference to undertake a review into Serious Invasions of Privacy in the Digital Era. On behalf of the Members of the Commission involved in this Inquiry, and in accordance with the *Australian Law Reform Commission Act 1996*, I am pleased to present you with the Final Report on this reference, Serious Invasions of Privacy in the Digital Era.

Yours sincerely,

Professor Rosalind Croucher
President

Professor Barbara McDonald
Commissioner in Charge

Contents

Terms of Reference **5**
Participants **7**
Recommendations **9**

Part 1 **15**

1. Introduction **17**
Context of the Inquiry 17
The design of a cause of action 18
Should a new tort be enacted? 20
Other reforms 26
The law reform process 27

2. Guiding Principles **29**
Summary 29
Principle 1: Privacy is a fundamental value worthy of legal protection 30
Principle 2: There is a public interest in protecting privacy 32
Principle 3: Privacy should be balanced with other important interests 33
Principle 4: Australian privacy laws should meet international standards 35
Principle 5: Privacy laws should be adaptable to technological change 36
Principle 6: Privacy laws should be clear and certain 36
Principle 7: Privacy laws should be coherent and consistent 37
Principle 8: Justice to protect privacy should be accessible 38
Principle 9: Privacy protection is an issue of shared responsibility 39

3. Overview of Current Law **41**
Summary 41
Existing legislative privacy protection 42
Existing common law causes of action 47
Filling the gaps in existing law 51
A common law action for breach of privacy in Australia? 53

Part 2 **57**

4. A New Tort in a New Commonwealth Act **59**
Summary 59
A new stand-alone Commonwealth Act 59
Constitutional issues 62
An action in tort 67
Abolition of common law actions 72

5. Two Types of Invasion **73**
Summary 73
A cause of action for two types of invasion of privacy 74
Intrusion upon seclusion 76
Misuse of private information 81
Examples 85
False light and appropriation 87
An open-ended action? 88
One cause of action, not two 89

6. Reasonable Expectation of Privacy **91**
Summary 91
A test for what is private 92
Considerations 96

7. Fault **109**
Summary 109
Intentional or reckless invasions of privacy 110
Negligence 118
Strict liability 124
Effect of apology on liability 128

8. Seriousness and Proof of Damage **131**
Summary 131
Seriousness 132
Proof of damage not required 138

9. Balancing Privacy with Other Interests **143**
Summary 143
The balancing exercise 144
Public interest matters 150
Onus of proof 158
A discrete exercise 161

10. Forums, Limitations and Other Matters **163**
Summary 163
Forums 164
Alternative dispute resolution processes 168
Cause of action limited to natural persons 171
Non-survival of the cause of action 172
Limitation periods 177
Young plaintiffs 181
First publication rule 182

11. Defences and Exemptions **185**
Summary 185
Lawful authority 186
Incidental to the exercise of a lawful right of defence of persons or property 191
Necessity 193

Consent 195
Absolute privilege 202
Publication of public documents 204
Fair report of proceedings of public concern 205
Safe harbour scheme for internet intermediaries 207
Exemption or defence for children and young persons 210
Defences unsuited to a privacy action 213

12. Remedies and Costs 219
Summary 219
Damages 220
Account of profits 238
No recommendation on notional licence fee 240
Injunctions 241
Delivery up, destruction or removal of material 251
Correction orders 252
Apology orders 254
Declarations 256
Costs 258

Part 3 261

13. Breach of Confidence Actions for Misuse of Private Information 263
Summary 263
The likely future development of the action for breach of confidence 264
Compensation for emotional distress 265
Public interest and injunction applications 273

14. Surveillance Devices 275
Summary 275
Existing surveillance device laws 276
A Commonwealth Act 278
Technology neutral surveillance legislation 282
Telecommunications surveillance 285
Participant monitoring 286
Responsible journalism and the public interest 289
Workplace surveillance 293
Remedial relief and compensation 295
Alternative forums for complaints about surveillance 296

15. Harassment 299
Summary 299
Statutory tort of harassment 300
Criminal offences for harassment 304
Harassment laws in other countries 307

16. New Regulatory Mechanisms **309**
Summary 309
Privacy Commissioner investigations for serious invasions of privacy 310
Amicus curiae and intervener functions 317
Deletion of personal information 319
Review of the small business exemption 321

Consultations **323**
Abbreviations **327**

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 Commissioner

The Hon Justice John Middleton, Federal Court of Australia

Executive Director

Sabina Wynn

Senior Legal Officer

Jared Boorer

Legal Officers

Dr Julie Mackenzie

Brigit Morris

Dr Steven Robertson

Legal Interns

Claire Bready

Ravi Gosal

Georgie Leahy

Alisha Mathew

Timothy Maybury

Michelle Meares

Jack Murray

Hagen Sporleder

Jackson Wherrett

Bradley Woods

Advisory Committee Members

The Hon Justice Peter D Applegarth, Supreme Court of Queensland

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 Hon W H Nicholas QC

Tara McNeilly, Senior General Counsel, Office of General Counsel, 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 Community, Faculty of Law, University of New South Wales

Acknowledgement

Research completed by the University of South Australia, 'Young People's Knowledge of and Attitudes toward Online Risks and Privacy':

Alexander Stretton

Larisa Karklins

Dr Barbara A Spears

Recommendations

4. A New Tort in a New Commonwealth Act

Recommendation 4–1 If a statutory cause of action for serious invasion of privacy is to be enacted, it should be enacted by the Commonwealth, in a Commonwealth Act (the Act).

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

5. Two Types of Invasion

Recommendation 5–1 The Act should provide that the plaintiff must prove that his or her privacy was invaded in one of the following ways:

(a) intrusion upon seclusion, such as by physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs; or

(b) misuse of private information, such as by collecting or disclosing private information about the plaintiff.

Recommendation 5–2 The Act should provide that 'private information' includes untrue information, but only if the information would be private if it were true.

6. Reasonable Expectation of Privacy

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

Recommendation 6–2 The 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, such as in the plaintiff's home;

(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, occupation and cultural background; and

(h) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy.

7. Fault

Recommendation 7–1 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.

Recommendation 7–2 The Act should provide that an apology made by the defendant does not constitute an admission of fault or liability and is not relevant to the determination of fault or liability.

8. Seriousness and Proof of Damage

Recommendation 8–1 The Act should provide that a plaintiff has an action under the new tort only where the invasion of privacy was 'serious', having regard, among other things, to:

(a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff; and

(b) whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff

Recommendation 8–2 The plaintiff should not be required to prove actual damage to have an action under the new tort.

9. Balancing Privacy with Other Interests

Recommendation 9–1 The Act should provide that, for the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest. A separate public interest defence would therefore be unnecessary.

Recommendation 9–2 The Act should include the following list of countervailing public interest matters which a court may consider, along with any other relevant public interest matter:

(a) freedom of expression, including political communication and artistic expression;

(b) freedom of the media, particularly to responsibly investigate and report matters of public concern and importance;

(c) the proper administration of government;

(d) open justice;

(e) public health and safety;

(f) national security; and

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

Recommendation 9–3 The Act should provide that the defendant has the burden of adducing evidence that suggests there is a countervailing public interest for the court to consider. The Act should also provide that the plaintiff has the legal onus to satisfy the court that the public interest in privacy outweighs any countervailing public interest that is raised in the proceedings.

10. Forums, Limitations and Other Matters

Recommendation 10–1 Federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy under the Act. Consideration should also be given to giving jurisdiction to appropriate state and territory tribunals.

Recommendation 10–2 The new tort should only be actionable by natural persons.

Recommendation 10–3 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.

Recommendation 10–4 A person should not be able to bring an action under the new tort after the earlier of:

(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.

Recommendation 10–5 In exceptional circumstances, the court may extend this limitation period, but the period should expire no later than six years from the date on which the invasion occurred.

Recommendation 10–6 Consideration should be given to extending the limitation period where the plaintiff was under 18 years of age when the invasion of privacy occurred.

Recommendation 10–7 Consideration should be given to enacting a 'first publication rule', also known as a 'single publication rule'. This would limit the circumstances in which a person may bring an action in relation to the publication of private information, when that same private information had already been published in the past.

11. Defences and Exemptions

Recommendation 11–1 The Act should provide for a defence that the defendant's conduct was required or authorised by law.

Recommendation 11–2 The 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.

Recommendation 11–3 The Act should provide for a defence of necessity.

Recommendation 11–4 The Act should provide for a defence of consent.

Recommendation 11–5 The Act should provide for a defence of absolute privilege.

Recommendation 11–6 The Act should provide for a defence of publication of public documents.

Recommendation 11–7 The Act should provide for a defence of fair report of proceedings of public concern.

Recommendation 11–8 The Act should provide for an exemption for children and young persons.

12. Remedies and Costs

Recommendation 12–1 The Act should provide that courts may award damages, including damages for emotional distress.

Recommendation 12–2 The Act should set out the following non-exhaustive list of factors that a court may consider when determining the amount of damages:

(a) whether the defendant had made an appropriate apology to the plaintiff;

(b) whether the defendant had published a correction;

(c) whether the plaintiff had already recovered compensation, or has agreed to receive compensation in relation to the conduct of the defendant;

(d) whether either party took reasonable steps to settle the dispute without litigation; and

(e) whether the defendant's unreasonable conduct following the invasion of privacy, including during the proceedings, had subjected the plaintiff to particular or additional embarrassment, harm, distress or humiliation.

Recommendation 12–3 The Act should provide that the court may not award a separate sum as aggravated damages.

Recommendation 12–4 The Act should provide that a court may award exemplary damages in exceptional circumstances.

Recommendation 12–5 The Act should provide for a cap on damages. The cap should apply to the sum of both damages for non-economic loss and any exemplary damages. This cap should not exceed the cap on damages for non-economic loss in defamation.

Recommendation 12–6 The Act should provide that a court may award an account of profits.

Recommendation 12–7 The Act should provide that the court may at any stage of proceedings grant an interlocutory or other injunction to restrain the threatened or apprehended invasion of privacy, where it appears to the court to be just or convenient and on such terms as the court thinks fit.

Recommendation 12–8 The Act should provide that, when considering whether to grant injunctive relief before trial to restrain publication of private information, a court must have particular regard to freedom of expression and any other matters of public interest.

Recommendation 12–9 The Act should provide that courts may order the delivery up and destruction or removal of material.

Recommendation 12–10 The Act should provide that courts may, where false private information has been published, order the publication of a correction.

Recommendation 12–11 The Act should provide that courts may order the defendant to apologise.

Recommendation 12–12 The Act should provide that courts may make a declaration.

13. Breach of Confidence Actions for Misuse of Private Information

Recommendation 13–1 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 plaintiff's emotional distress.

14. Surveillance Devices

Recommendation 14–1 The Commonwealth Government should enact surveillance legislation to replace existing state and territory surveillance device laws.

Recommendation 14–2 Surveillance legislation should be technology neutral. It should regulate surveillance through the use of listening devices, optical devices, tracking devices, data surveillance devices, and other devices and systems.

Recommendation 14–3 The Commonwealth Government should consider consolidating telecommunications surveillance laws with the new Commonwealth surveillance legislation.

Recommendation 14–4 Surveillance legislation should not contain a defence or exception for participant monitoring.

Recommendation 14–5 Surveillance legislation should provide a defence for responsible journalism relating to matters of public concern and importance.

Recommendation 14–6 Workplace surveillance laws should be made uniform throughout Australia.

Recommendation 14–7 Surveillance legislation should provide that a court may order remedial relief, including compensation, for a person subjected to unlawful surveillance.

Recommendation 14–8 State and territory governments should give jurisdiction to appropriate courts and tribunals to hear complaints about the installation and use of surveillance devices that can monitor neighbours on residential property.

15. Harassment

Recommendation 15–1 If a statutory cause of action for serious invasion of privacy is not enacted, state and territory governments should enact uniform legislation creating a tort of harassment.

16. New Regulatory Mechanisms

Recommendation 16–1 The Commonwealth Government should consider extending the Privacy Commissioner's powers so that the Commissioner may investigate complaints about serious invasions of privacy and make appropriate declarations. Such declarations would require referral to a court for enforcement.

Recommendation 16–2 The following functions should be conferred on the Privacy Commissioner:

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

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

Part 1

1. Executive Summary

Contents

Context of the Inquiry 17
The design of a cause of action 18
Elements and essential features of the tort 18
Limitation periods and other matters 19
Defences 19
Remedies 20
Should a new tort be enacted? 20
International developments 22
A common law or statutory tort? 23
Other inquiries 25
Other reforms 26
Breach of confidence 26
Surveillance 26
Harassment 27
Regulation 27
The law reform process 27

Context of the Inquiry

1.1 A cause of action for serious invasion of privacy does not presently exist in Australian law. A person's privacy may be invaded in a range of ways. Such invasions may occur with increasing ease and frequency in the digital era, when the mobile phones in our pockets are all potential surveillance devices, drones are becoming cheaper and more advanced, and personal information once put online seems impossible to destroy or forget.[1]

1.2 This Inquiry considers how Australian law may be reformed to prevent and remedy serious invasions of privacy. However, it occurs in the context of other concerns about privacy, such as those raised by 'big data' and surveillance by governments and others. Indeed, it seems that privacy is rarely out of the news.

1 This has been called the problem of 'digital eternity': David Lindsay, 'The "Right to Be Forgotten" in European Data Protection Law', *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 290, 293.

The design of a cause of action

1.3 The Report sets out the detailed legal design of a statutory civil cause of action for serious invasion of privacy. This was the core task given to the ALRC for this Inquiry.[2]

1.4 Notably, the cause of action designed in the Report is directed at invasions of privacy that are serious, committed intentionally or recklessly, and that cannot be justified in the public interest. It is also confined to invasions of privacy either by intrusion upon seclusion or by misuse of private information.

1.5 The design of this action and the other recommendations in the Report were informed by nine guiding principles, discussed in Chapter 2. These include the principle that privacy is a fundamental value worthy of legal protection and an important public interest.

1.6 Another principle is that privacy should be balanced with other rights and interests, such as freedom of expression. The ALRC considers that privacy and free speech are both better protected by finding a reasonable balance between them.

1.7 The cause of action is designed in detail in the Report. This should make more clear the scope of the action, the extent of protection it may provide, and the impact it may have on potential defendants. The detailed design of the cause of action may also help better inform debates about the desirability of such a cause of action.

1.8 In developing its recommendations, the ALRC considered, among other things, common law principles, developments in other jurisdictions, gaps in Australian common law and statute law, and recommendations made in previous inquiries into privacy law. The ALRC also considered community and industry concerns, including about threats to privacy by new technologies and the vital importance of free speech.

Elements and essential features of the tort

1.9 The cause of action should be enacted in a Commonwealth Act and should be described in the statute as an action in tort. This is the first essential feature of the cause of action. Chapter 4 sets out the constitutional background and legal implications of this recommendation. Importantly, describing the action as a tort will encourage courts to draw on established principles of tort law, when deciding a number of ancillary issues. This will provide a measure of certainty, consistency and coherence to the law.

1.10 Chapters 5 to 8 set out the elements and essential features of the tort. The overall structure and elements of the cause of action should be read together, as each element depends in many ways on the existence of the others.

---

2 See the Terms of Reference.

1.11 These are the essential elements and features of the cause of action:

- the invasion of privacy must be either by intrusion into seclusion or by misuse of private information (Chapter 5);
- it must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances (Chapter 6);
- the invasion must have been committed intentionally or recklessly—mere negligence is not sufficient (Chapter 7);
- the invasion must be serious (Chapter 8);
- the invasion need not cause actual damage, and damages for emotional distress may be awarded (Chapter 8); and
- the court must be satisfied that the public interest in privacy outweighs any countervailing public interests (Chapter 9).

1.12 This last point is the crucial 'balancing exercise', in which courts weigh privacy against other important public interests, such as freedom of speech, freedom of the media, public health and safety, and national security. The ALRC recommends that such competing interests be considered when determining whether the plaintiff has a cause of action. It should be an element of the tort, rather than a defence. A plaintiff should not be able to claim that a wrong has been committed—that their privacy has been seriously invaded—where there are strong public interest grounds justifying the invasion of privacy.

Limitation periods and other matters

1.13 Chapter 10 deals with important procedural and substantive matters. The ALRC recommends that:

- federal, state and territory courts should have jurisdiction;
- the cause of action should be limited to natural persons;
- actions should not survive—either for the estate of the plaintiff or against the estate of the defendant;
- the limitation period should be set at one year after the plaintiff becomes aware of the invasion, or three years after the invasion occurred, whichever comes first; and
- alternative dispute resolution should neither be a bar to, nor a prerequisite for, litigation.

Defences

1.14 Chapter 11 sets out the recommended defences to the cause of action:

- a defence of lawful authority;
- a defence where the conduct was incidental to defence of persons or property;

- a defence of consent;
- a defence of necessity;
- a defence of absolute privilege;
- a defence for the publication of public documents; and
- a defence for fair reporting of public proceedings.

Remedies

1.15 Chapter 12 discusses the making of costs orders and sets out the monetary and non-monetary remedies that should be available for serious invasions of privacy, including:

- damages, including for emotional distress and, in exceptional circumstances, exemplary damages;
- an account of profits;
- injunctions;
- delivery up, destruction and removal of material;
- correction and apology orders; and
- declarations.

1.16 The ALRC also recommends a list of factors for courts to consider in assessing damages and that there should be a statutory cap on the amount of damages that may be awarded in any particular case.

Should a new tort be enacted?

1.17 The ALRC was asked to design a cause of action, rather than to determine whether it is needed or desirable. This second question was considered and answered affirmatively by three recent law reform inquiries in Australia. It was also the subject of an Issues Paper prepared by the Department of Prime Minister and Cabinet in September 2011.[3] Nevertheless, many stakeholders in this Inquiry commented on the issue.

1.18 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 should be assessed on the basis of an understanding of:

- the existing legal protections for privacy;
- gaps and deficiencies in that legal protection;

3 See below, [1.41] ff.

- the likelihood of the common law developing a cause of action for invasions of privacy in the absence of a statute;
- the detailed design of the cause of action—its elements, defences and remedies; and
- whether the cause of action is better designed in statute, or left to be developed by the courts.

1.19 Many stakeholders expressed their support for a statutory cause of action.[4] Only a few 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.[5] Even many of those who opposed a privacy tort did not deny the importance or value of privacy.[6] Rather, they based their opposition to the tort on other grounds. It was said that there was little evidence that privacy is invaded in Australia, and that there are no media practices in Australia such as those exposed in the UK phone hacking scandal involving the now defunct *News of the World*. It was also said that there are no significant gaps in the law, and a new tort would have an undesirable effect on the media, on other businesses, and on the free flow of information.

1.20 The ALRC is not convinced that there is no evidence of invasions of privacy in Australia. Invasions of privacy by intrusion or misuse of private information are known to occur in a wide variety of circumstances.

1.21 While it may be true that the Australian media operate more appropriately than some of their UK counterparts, it is not necessarily the case that the Australian media never unjustifiably invade people's privacy. Rather, it may be that where they have done so, and the plaintiff complains, they have settled the plaintiff's claims to avoid litigation, publicity and the setting of a precedent.

1.22 The fact that courts have not recognised a common law cause of action, as they have in other countries, also does not show that there is no need for a statutory cause of action. It may merely indicate that litigants are reluctant to risk lengthy and costly proceedings and appeals arguing a novel point of law. ALRC consultations with practitioners confirmed this view.

1.23 Some who opposed the introduction of a new cause of action recognised that there are gaps in the law, but submitted that it would be preferable to fill those gaps in other ways.[7] Other stakeholders who opposed a new privacy tort submitted that it

---

4 Law Society of NSW, *Submission 122*; N Witzleb, *Submission 116*; Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; N Henry and A Powell, *Submission 104*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Sex Party, *Submission 92*; G Greenleaf, *Submission 76*; M Paterson, *Submission 60*.

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

6 Media and Communications Committee of the Law Council of Australia, *Submission 124*; AMTACA, *Submission 101*.

7 Telstra, *Submission 107*; Australian Bankers' Association, *Submission 84*; Guardian News and Media Ltd and Guardian Australia, *Submission 80*; P Wragg, *Submission 73*; SBS, *Submission 59*; AIMIA Digital Policy Group, *Submission 56*; News Corp Australia, *Submission 34*.

would nevertheless be preferable to 'shoehorning' privacy protection into existing actions.[8]

International developments

1.24 There are civil causes of action for serious invasion of privacy in New Zealand, the United Kingdom, the United States and Canada.

1.25 The UK 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).[9] This Act requires the courts to give effect to the protection of rights and freedoms in the *European Convention on Human Rights*.

1.26 Article 8 of the *Convention* provides that everyone has the right to respect for their private and family life, their home and their correspondence, and that there shall be no interference with this right by a public authority except by lawful authority in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. Article 10 provides that everyone has the right to freedom of expression, subject to certain necessary restrictions, including the protection of the reputation or rights of others, and the prevention of disclosure of confidential information.

1.27 This UK action for disclosure of private information—sometimes called a tort—has provided a useful guide to the possible structure of the statutory cause of action designed in the Report. The UK has also enacted the *Protection from Harassment Act 1997* (UK), which provides a civil remedy for harassment.[10]

1.28 New Zealand courts have recognised common law torts of misuse of private information[11] and of intrusion.[12] New Zealand has enacted the *Harassment Act 1997* (NZ), which provides criminal penalties for harassment.

1.29 Although committees in the UK and New Zealand have recommended against the introduction of a statutory cause of action,[13] this must be seen in light of the significant and recent developments in the common law in those two countries.

1.30 The Canadian provinces of British Columbia,[14] Manitoba,[15] Newfoundland and Labrador,[16] Quebec[17] and Saskatchewan[18] have enacted statutory torts for invasion of

---

8 Guardian News and Media Ltd and Guardian Australia, *Submission 80*.
9 *Campbell v MGN Ltd* [2004] 2 AC 457. See Ch 12.
10 See Ch 15.
11 *Hosking v Runting* (2005) 1 NZLR 1.
12 *C v Holland* [2012] 3 NZLR 672.
13 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).
14 *Privacy Act*, RSBC 1996, c 373 (British Columbia).
15 *Privacy Act*, CCSM 1996, c P125 (Manitoba).
16 *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador).
17 *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35–37.
18 *Privacy Act*, RSS 1978, c P-24 (Saskatchewan).

privacy, and the Ontario Court of Appeal has also recognised common law protection.[19]

1.31 Privacy torts have been well-established in the United States for many decades, although the protection they provide is limited by the special protection given to free speech by the First Amendment of the *Constitution*. Some states, such as California, have also introduced a statutory tort of invasion of privacy.[20]

A common law or statutory tort?

1.32 In contrast to these other jurisdictions, a common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility 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. In Chapter 3, the ALRC reviews the relevant case law, but agrees with the general consensus that the direction of the future development of the common law is difficult to predict.[23]

1.33 However, Australian law is unlikely to stand still, given developments in other countries with similar legal systems and principles. Although Australia does not have a Human Rights Act, Australia is a signatory to the *International Covenant on Civil and Political Rights*, which requires countries to protect the privacy of its citizens. Privacy is also grounded in clear and important common law principles. Professor Eric Barendt has noted that in the 18th century, property rights that would now be identified as personal privacy interests, 'were used to safeguard radicals against the arbitrary confiscation of their manuscripts and papers'.[24] It will be increasingly difficult to justify denying legal redress to people whose privacy has been seriously invaded, when other countries offer such redress.

1.34 If a cause of action for serious invasion of privacy is likely to be developed in Australia, is it better enacted by parliament, or left for the courts to develop under the common law? There are benefits of having the law develop in the courts. A statute can have unintended consequences.[25] It may capture, or fail to capture, activities or conduct that were not considered when the statute was enacted. A statute may also become outdated by changes in social or technological changes.[26] A court, on the other hand, can only decide the case before it, and only the issues in contention between the

---

19 *Jones v Tsige* (2012) ONCA 32.

20 *California Civil Code* § 1708.8.

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 Eric Barendt, 'Privacy and Freedom of Speech' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006) 11, 31.

25 TT Arvind and Jenny Steele (eds), *Tort Law and the Legislature: Common Law, Statute and the Dynamics of Legal Change* (Hart Publisher, 2013) 8.

26 SBS, Submission No 8 to DPM&C Issues Paper, 2011; Free TV, *Submission 55*.

parties. It does not need to anticipate or resolve all the possible issues that might arise in other cases. The common law may therefore develop more incrementally and, some would say, cautiously.

1.35 However, there are also many benefits of statutory reform. Parliament can act on its own motion, and proactively address emerging issues in the community. The development of the common law depends on the existence of parties with the will, and the necessary resources, to litigate their claim in court.[27] There will be continuing uncertainty about how the law will be developed in the courts.[28] Reform by legislation can also be effected more rapidly than development at common law.[29]

1.36 A statute can legislate for a range of situations, both for what has occurred in the past and for what may happen in the future. A court will focus on the specific issues of a particular case, and this may lead to the development of narrow, fact-specific legal principles.

1.37 There is more flexibility in the development of the law by statute than by common law. Statute is not bound to follow precedent, unlike the courts.

1.38 Statutes can also select the most appropriate elements of a cause of action, remedies, defences, thresholds, caps, conditions and exceptions, while courts often do not have this freedom.[30] A statute can also build in incentives to use alternative dispute resolution processes.

1.39 Finally, statutes can address the complex policy issues and legal concepts involved and express the law in language which is more accessible than case law for people without legal training.[31] As a result, statutes may be more effective in having a normative impact on behaviour.

1.40 The advantages of statutory reform should not be underestimated by those who oppose a new privacy tort. If instead of statutory reform, the equitable action for breach of confidence were extended, defendants may be faced with a much stricter standard of liability. There may also not be a clear and separate 'seriousness' threshold and countervailing public interests may not be given sufficient weight. Such things considered, potential defendants may prefer a more targeted statutory tort, such as the one designed in the Report.

---

27 Office of the Victorian Privacy Commissioner, Submission No 46 to DPM&C Issues Paper, 2011; Australian Privacy Foundation, Submission No 7 to DPM&C Issues Paper, 2011.

28 Law Council of Australia, Submission No 55 to DPM&C Issues Paper, 2011; Office of the Australian Information Commissioner, Submission No 14 to DPM&C Issues Paper, 2011.

29 Australian Privacy Foundation, Submission No 7 to DPM&C Issues Paper, 2011; Liberty Victoria, Submission No 34 to DPM&C Issues Paper, 2011.

30 Mark Leeming, 'Theories and Principles Underlying the Development of the Common Law: The Statutory Elephant in the Room' (2013) 36 *UNSW Law Journal* 1002, 1021.

31 M Paterson, *Submission 60*.

Other inquiries

1.41 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.[32]

1.42 The ALRC's 2008 Report, *For Your Information: Privacy Law and Practice*, 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.[33]

1.43 In 2009, the New South Wales Law Reform Commission recommended that a general cause of action for invasion of privacy was required to provide a 'basis for the ongoing development of the law of privacy in a climate of dynamic societal and technological change'.[34]

1.44 In 2010, the Victorian Law Reform Commission issued the report, *Surveillance in Public Places*, which followed a decade-long inquiry into workplace privacy and privacy in public places.[35]

1.45 In September 2011, the Department of the Prime Minister and Cabinet released an Issues Paper on a statutory cause of action for invasion of privacy,[36] prompted by a number of 'high profile privacy breaches' in Australia and overseas.[37]

1.46 During this Inquiry, the Law Reform Institute of South Australia has initiated an Inquiry into whether or not South Australia should enact a statutory cause of action for invasion of privacy.[38]

---

32 Privacy was also the subject of earlier reports by the ALRC. In 1979, the ALRC recommended that a person be allowed to sue for damages or an injunction if 'sensitive private facts' were published in circumstances that were likely to cause distress, annoyance or embarrassment to a person in the position of the relevant individual: Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, Report 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: Australian Law Reform Commission, *Privacy*, Report 22 (1983). This resulted in the enactment of the *Privacy Act 1988* (Cth). In the latter report at [1081], the ALRC declined to recommend the creation of a general tort of invasion of privacy. In the ALRC's view at that time, 'such a tort would be too vague and nebulous'. The ALRC considers that not only are social and technological conditions 30 years later very different, but also the legal landscape has changed considerably, as shown by developments in other countries discussed above.

33 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–1.

34 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [4.14].

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

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

37 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).

38 South Australian Law Reform Institute, *Too Much Information: A Statutory Cause of Action for Invasion of Privacy*, Issues Paper 4 (2013).

1.47 The Law Reform Committee of Victoria also recommended in early 2013 that Victoria give further consideration to introducing a statutory cause of action for invasion of privacy by the misuse of private information.[39]

Other reforms

1.48 In addition to designing the statutory cause of action, the ALRC was asked to make recommendations about other legal remedies and innovative ways in which the law could prevent or redress serious invasions of privacy. This is considered in Part 3 of the Report.

Breach of confidence

1.49 Chapter 13 recommends that, if a statutory cause of action for serious invasion of privacy is not enacted, the equitable action for breach of confidence be strengthened by legislation enabling courts to award compensation for emotional distress. As noted in Chapter 3, compensation for emotional distress, falling short of a recognised psychiatric illness, is generally not available for breach of confidence. If a statutory cause of action for serious invasion of privacy is not enacted, enabling courts to award compensation for emotional distress in such cases would provide an important mechanism for redress.

Surveillance

1.50 Chapter 14 concerns legislation regulating the use of surveillance devices. Existing state and territory laws provide important protection of privacy and related rights—such as freedom of speech—however there is significant inconsistency in the law between jurisdictions. This inconsistency can make the laws less effective, undermining privacy, and it can also be costly for businesses that operate nationally. The ALRC considers that surveillance device laws should be the same throughout Australia, and recommends that Commonwealth legislation be enacted to replace existing state and territory laws.

1.51 Surveillance legislation should also be technology neutral, so that the law can apply to new devices, such as unmanned aerial vehicles (drones), as well as to surveillance technologies which are not 'devices' in the traditional sense, such as software or networks of devices. The ALRC also questions the value of the existing distinction built into the law between surveillance using a device and surveillance using a communications network.[40]

1.52 A 'responsible journalism' defence to surveillance laws is also recommended, to protect journalists and media groups who make appropriate use of a surveillance device for journalism in the public interest.

---

39 Law Reform Committee, Parliament of Victoria, *Inquiry into Sexting* (2013) 187–8.

40 The Senate Standing Committee on Legal and Constitutional Affairs is conducting a comprehensive review of the *Telecommunications (Interception and Access) Act 1979* (Cth). It is due to report in August 2014.

Harassment

1.53 Chapter 15 recommends that, if a statutory cause of action for serious invasion of privacy is not enacted, state and territory governments should enact uniform legislation providing for a statutory tort of harassment. A tort of harassment, based on similar laws in other jurisdictions, would provide protection and redress for individuals who experience some of the most serious invasions of privacy. The ALRC also highlights some gaps in state, territory and Commonwealth criminal offences for harassment.

Regulation

1.54 Chapter 16 considers limited reforms to the existing regulatory mechanisms for protecting privacy. In particular, the ALRC recommends that the existing powers of the Privacy Commissioner to investigate breaches of the *Privacy Act 1988* (Cth) be extended to allow investigations of complaints about serious invasions of privacy more generally. This would provide a low-cost avenue for individuals to make complaints about serious invasions of privacy. The ALRC also recommends that the Commissioner be given the additional functions of amicus curiae or intervener in relevant court proceedings.

The law reform process

1.55 The ALRC was given Terms of Reference in June 2013 and asked to report to the Attorney-General by June 2014. These Terms of Reference set out and limit the scope of the ALRC's Inquiry.

1.56 The Report is the final stage in the process. The first stage included the release of an Issues Paper,[41] and the second stage was a Discussion Paper.[42]

1.57 Many valuable submissions to both papers were received.[43] The ALRC also conducted a number of consultations with stakeholders and spoke at public and industry forums and conferences. The ALRC met with media, telecommunications, social media and marketing companies, among other organisations; many expert academic commentators, specialist legal practitioners, and judges; public interest groups; and government agencies, including the Office of the Australian Information Commissioner, the Australian Communications and Media Authority, and the Australian Human Rights Commission.[44] The ALRC hosted two roundtables of legal experts, in Sydney and London.

1.58 In addition to the contribution of expertise by way of consultations and submissions, specific expertise is also received by the ALRC from members of its Advisory Committee and the appointment of part-time Commissioners.

---

41 *Serious Invasions of Privacy in the Digital Era* (ALRC IP 43, 2013).

42 *Serious Invasions of Privacy in the Digital Era* (ALRC DP 80, 2014). The Report, the Issues Paper and the Discussion Paper may all be downloaded free of charge from the ALRC website: <www.alrc.gov.au>. Hard copies may be obtained on request by contacting the ALRC on (02) 8238 6333.

43 Public submissions are also published on the ALRC website: <www.alrc.gov.au>.

44 A list of consultations is set out at the end of the Report.

1.59 The role of the Advisory Committee is to advise on the coherence and structure of the ALRC process and recommendations; it does not formulate reform recommendations, and members are invited in their individual capacity. They are explicitly asked not to act in any representative capacity.

1.60 The ALRC acknowledges the contribution made by all the part-time Commissioners, Advisory Committee members and expert readers in this Inquiry and expresses gratitude to them for voluntarily providing their time and expertise.[45]

1.61 The Report discharges the tasks given to the ALRC in the Terms of Reference: to design a statutory cause of action for serious invasion of privacy, and to recommend other ways the law might be reformed to deter and redress serious invasions of privacy. The ALRC considers that the recommendations in the Report, if enacted, would fill an increasingly conspicuous gap in Australian law. They would help protect the privacy of Australians, while respecting and reinforcing other fundamental rights and values, including freedom of expression.

45 The names of Commissioners and Advisory Committee members appears at the front of the Report.

2. Guiding Principles

Contents

Summary 29
Principle 1: Privacy is a fundamental value worthy of legal protection 30
Principle 2: There is a public interest in protecting privacy 32
Principle 3: Privacy should be balanced with other important interests 33
Principle 4: Australian privacy laws should meet international standards 35
Principle 5: Privacy laws should be adaptable to technological change 36
Principle 6: Privacy laws should be clear and certain 36
Principle 7: Privacy laws should be coherent and consistent 37
Principle 8: Justice to protect privacy should be accessible 38
Principle 9: Privacy protection is an issue of shared responsibility 39

Summary

2.1 The ALRC has identified nine principles to guide the recommendations for reform in this Inquiry. The principles are not designed to limit the scope of the Inquiry, but rather to assist the ALRC, governments and other stakeholders, by providing a policy framework in which to consider options for reform of the law.

2.2 The principles are not the only matters considered by the ALRC, but they generally accord with widely recognised values and concepts that have been set out in discussions about the legal protection of privacy.

2.3 Stakeholders expressed general support for these principles.[1] Some stakeholders suggested additional matters that should be incorporated; 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.

2.4 Discussion among government representatives, law practitioners, commentators, researchers and others into the value, importance and role of privacy in various contexts and from various perspectives—legal, philosophical, social, political, technical—is extensive. This chapter identifies key considerations from the literature that underpin the recommendations in this Final Report.

---

1 ASTRA, *Submission 99*; SBS, *Submission 59*; Women's Legal Services NSW, *Submission 57*; Google, *Submission 54*; Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; Australian Bureau of Statistics, *Submission 32*; Public Interest Advocacy Centre, *Submission 30*; Insurance Council of Australia, *Submission 15*.

2.5 The principles draw on leading cases in Australia and other comparable jurisdictions, international conventions, academic commentary on privacy and related fields, the Terms of Reference for this Inquiry, 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 fundamental to our understanding and appreciation of personal identity and freedom.[2] Privacy underpins:

- meaningful and satisfying interpersonal relationships, including intimate and family relationships;
- freedom of speech, thought and self-expression;
- freedom of movement and association;
- engagement in the democratic process;
- freedom to engage in secure financial transactions;
- freedom to pursue 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.[3] 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.[4]

2.8 One challenge which arises when determining the boundaries for greater privacy protection is drawing the difficult distinction between the public and the private spheres. In *ABC v Lenah Game Meats,* Gleeson CJ stated that

> 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.[5]

---

2 Jon L Mills, *Privacy: The Lost Right* (Oxford University Press, 2008) 13.

3 *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.

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

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

2.9 There is no doubt that privacy is a complex concept, difficult to define at a conceptual level.[6] It has even been said to be dogged by a 'lack of precision'[7] and possibly 'more akin to a 'bundle of rights'.[8] However, privacy is not less valuable or deserving of legal protection simply because it is hard to define. The New South Wales Law Reform Commission said that to suggest that privacy is impossible to protect because it cannot be precisely defined is to 'succumb to what Lord Reid once described as "the perennial fallacy that because something cannot be cut and dried or lightly weighed or measured therefore it does not exist"'.[9]

2.10 In 1890, Professors Samuel Warren and Louis Brandeis famously described privacy as the 'right to be let alone'.[10] In the United States (US), the development of privacy is also closely aligned with protection of autonomy,[11] and privacy has been understood to include the right to make choices and exercise personal liberties.[12]

2.11 There is debate about whether privacy should be expressed as a value, a right or an interest. The Office of the Australian Information Commissioner (OAIC) argued that privacy should be reframed as a right.[13] In *ABC v Lenah Games Meats,* Gleeson CJ drew a distinction between legal 'rights' and 'legal interests', suggesting that

> talk of 'rights' may be question-begging, especially in a legal system which has no counterpart to the First Amendment to the United States Constitution or to the *Human Rights Act 1998* of the United Kingdom. The categories that have been developed in the United States for the purpose of giving greater specificity to the kinds of interest protected by a 'right to privacy' illustrate the problem.[14]

2.12 Jurisprudence from the European Court of Human Rights has developed a broad understanding of privacy in the context of art 8 of the European Convention on Human Rights. Article 8 has been interpreted to protect an individual's correspondence, including through modern communication techniques such as email,[15] physical integrity,[16] home,[17] identity,[18] personal autonomy[19] and personal development.[20]

2.13 Many stakeholders stressed the importance of privacy to a person's autonomy and rights of self-determination.[21] The Law Institute of Victoria, for example, noted

---

6 Raymond Wacks, 'The Poverty of Privacy' (1980) 96 *Law Quarterly Review* 73.
7 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [41] (Gleeson CJ).
8 Mills, above n 2, 4.
9 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [4.16], quoting Lord Reid in *Ridge v Baldwin* [1964] AC 40, 64–65.
10 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
11 Mills, above n 2, 15.
12 Ibid 4.
13 Office of the Australian Information Commissioner, *Submission 66*.
14 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [41].
15 *Copland v UK* (2007) 45 EHRR 37.
16 *YF v Turkey* (2004) 39 EHHR 34.
17 *Keegan v UK* (2007) 44 EHRR 112.
18 *I v UK* (2003) 36 EHRR 53.
19 *Rotaru v Romania* (2000) 8 EHRR 449.
20 *Gaskin v UK* (1989) 12 EHRR 36. See, Ian Walden and Lorna Woods, 'Broadcasting Privacy' (2011) 3 *Journal of Media Law* 117, 125.
21 See, eg, Electronic Frontiers Australia, *Submission 44*; A Johnston, *Submission 9*; I Pieper, *Submission 6*.

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'.[22]

2.14 Privacy also gives individuals freedom to pursue 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 Islander people, who have particular cultural identity, knowledge and customs that bear on the privacy interests of individuals within the group.[23]

2.15 Some representative groups stressed the importance of a right to privacy for protecting vulnerable people in the community.[24] Associate Professor Moira Paterson emphasised the potential impact of surveillance on vulnerable people who may rely on public places as social, living and cultural spaces.[25] Protecting privacy can play an important role in ensuring personal safety and freedom from harassment.

Principle 2: There is a public interest in protecting privacy

2.16 While privacy must sometimes be set aside for broader public interests, privacy itself is also a vital public interest. The 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 protecting and enforcing private freedoms, rights and interests.[26] In *Plenty v Dillon,* Gaudron and McHugh JJ said:

> 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.[27]

2.17 Contractual and equitable obligations of confidence also have public interest justifications.[28] In the *Spycatcher* case, Lord Goff noted that

> the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law[29]

2.18 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

---

22 Law Institute of Victoria, *Submission 22*.
23 Arts Law Centre of Australia, *Submission 43*.
24 Women's Legal Services NSW, *Submission 57*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*.
25 M Paterson, *Submission 60*.
26 Australian Privacy Foundation, *Submission 110*; UNSW Cyberspace Law and Policy Community, *Submission 98*.
27 *Plenty v Dillon* (1991) 171 CLR 635, 655 (Gaudron and McHugh JJ).
28 On the public interest in upholding confidences, see *Prince of Wales v Associated Newspapers Ltd* [2007] 3 WLR 222, [67]. See Ch 12.
29 *Attorney General v Guardian Newspapers Ltd (No 2) (Spycatcher)* [1988] 1988 UKHL 6, 29 (Lord Goff).

to speak freely and honestly about important private matters, such as private sexual or medical matters.

2.19 There is a public interest in the security of confidential information about an individual's financial and commercial interests. There is, for example, a public interest in the benefits that online trade and commerce can offer. Respecting privacy helps establish consumer trust in these services. The preamble to the Asia-Pacific Economic Cooperation Privacy Framework states that balancing and promoting effective information privacy protection and the free flow of information is 'a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce'.[30]

2.20 Protecting privacy also has an important role to play in protecting and promoting free speech—another vital public interest. Professor Eric Barendt has written:

> One value of privacy, and a reason why it is recognised as a constitutional or legal right, is that it gives individuals the space to develop their own identity by themselves, and in communication and cooperation with friends and lovers, free from observation and interference by Big Brother or even by a liberal democratic state. Some privacy is essential to enable us to read, contemplate and formulate thoughts, and some confidentiality and security is similarly necessary to exchange ideas with friends and colleagues.[31]

2.21 Although privacy has been said to lie at the heart of liberty, and will often support other fundamental rights and freedoms, sometimes it must be balanced with other important interests.

Principle 3: Privacy should be balanced with other important interests

2.22 The privacy of an individual is not an absolute value or right that necessarily takes precedence over other values of public interest. As many stakeholders noted, it must be balanced with a range of other important values, freedoms and matters of public interest.[32] These may include, in no particular order or hierarchy:

- freedom of speech,[33] including the freedom of the media and the implied constitutional freedom of political communication;[34]
- freedom of artistic and creative expression and innovation in the digital era;[35]

---

30 Asia-Pacific Economic Cooperation, APEC Privacy Framework (2005) [1].

31 Eric Barendt, 'Privacy and Freedom of Speech' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006) 11, 30–31.

32 Australian Human Rights Commission, *Submission 75*; SBS, *Submission 59*; Google, *Submission 54*; ASTRA, *Submission 47*; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*.

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

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

35 Facebook, *Submission 65*.

- the public's right to be informed on matters of public importance, in real time rather than after delay;[36]
- public access to information and accurate historical records;[37]
- 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;[38]
- the effective delivery of essential and emergency services in the community;[39]
- the protection of vulnerable persons in the community;
- the right to be free from violence, including family violence;[40]
- national economic development and participation in the global digital economy;[41]
- the social and economic value of analysing 'big data';[42]
- the free flow of information and the right of business to achieve its objectives efficiently;[43] and
- the value of individuals being enabled to engage in digital communications and electronic financial and commercial transactions.[44]

2.23 The importance of balancing privacy with other important public interests underpins all the recommendations in this Report. The ALRC does, however, recognise

---

36 ASTRA, *Submission 47*.

37 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, 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: *Archives Act 1983* (Cth) s 33(1)(g).

38 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. See also Australian Federal Police, *Submission 67*; Google, *Submission 54*; CV Check, *Submission 23*; Insurance Council of Australia, *Submission 15*.

39 Australian Communications and Media Authority, *Submission 52*.

40 Women's Legal Services NSW, *Submission 115*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*.

41 Google, *Submission 54*; Telstra, *Submission 45*; Optus, *Submission 41*; Australian Bankers' Association, *Submission 27*.

42 See, eg, Malcolm Turnbull MP, 'National Archives Conference Address—Open for Business in the Digital Economy' (2 June 2014).

43 Australian Bankers' Association, *Submission 27*.

44 CV Check, *Submission 23*.

that privacy should not be casually 'traded off' for the sake of other important interests.[45]

Principle 4: Australian privacy laws should meet international standards

2.24 The protection of individual privacy in Australia should be consistent with Australia's international obligations.[46] These include Australia's obligations under the ICCPR[47] and policies of the Organisation for Economic Co-operation and Development.[48] It should also take into account, as far as appropriate, international standards and legal developments in the protection of privacy.[49] Human rights frameworks in Victoria and the ACT make specific reference to a person's right to privacy.[50]

2.25 Throughout this Report, reference is made to developments in the legal protection of privacy in other jurisdictions—particularly those with which Australia shares a common legal heritage. However, the ALRC 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.[51] The need for statutory reform in a particular jurisdiction also depends on developments in the common law.

2.26 Women's rights organisations highlighted the relevance of the International Covenant on the Elimination of All Forms of Violence Against Women (CEDAW)[52] to a new privacy tort. The disclosure of sexually explicit images of people without their consent by current or former intimate partners—'revenge pornography'—is one type of violence against women raised by several stakeholders.[53]

2.27 The Arts Law Centre of Australia said Indigenous culture and intellectual property should be recognised in the guiding principles:

> Any law protecting the privacy of individuals should also consider the confidential or culturally sensitive nature of cultural knowledge, stories, images of Indigenous Australians.[54]

---

45 Public Interest Advocacy Centre, *Submission 30*.

46 One of the ALRC's functions is to recommend reforms consistent with Australia's international obligations: *Australian Law Reform Commission Act 1996* (Cth) s 24(1)(b).

47 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) arts 17, 19.

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

49 Australian Bureau of Statistics, *Submission 32*.

50 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(a); *Human Rights Act 2004* (ACT) s 12.

51 SBS, *Submission 59*.

52 *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).

53 Women's Legal Services NSW, *Submission 57*.

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

2.28 Some stakeholders noted the value in constructing privacy law which is consistent with best practice in international standards, particularly in the area of data protection.[55]

2.29 International law recognises the importance of other rights and interests, such as freedom of speech. As noted in Principle 3, privacy must often be balanced with these other important rights and interests.

Principle 5: Privacy laws should be adaptable to technological change

2.30 The design of any legal privacy protection should be sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments. At the same time, laws should be drafted with sufficient precision and definition to promote certainty as to their application and interpretation.

2.31 Several stakeholders stressed the need for law reform to be technologically neutral to avoid laws being rendered obsolete by rapid developments in technology.[56] 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:

> policymakers need to understand the power of data, embrace its utility, and carefully address the challenges it raises without sacrificing the potential it offers.[57]

2.32 The importance of flexibility and adaptability is reflected in the design of the statutory cause of action and the reforms to surveillance laws recommended in this Report.

Principle 6: Privacy laws should be clear and certain

2.33 The law should be precise and certain, while being flexible and adaptable to changes in social and technological conditions. This principle underpins all of the ALRC's recommendations. Many stakeholders stressed the benefits of precision, clarity and certainty.[58]

2.34 The ALRC is mindful that Parliament cannot legislate precisely for all future situations. Courts will need to apply broader principles and weigh competing interests, in the light of all the circumstances of a particular case. Stakeholders pointed out that judges are familiar with deciding the types of issues that will arise in privacy cases,

---

55 Google, *Submission 54*.

56 Ibid; 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*.

57 Google, *Submission 54*.

58 ASTRA, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*; C Jansz-Richardson, *Submission 24*.

such as the existence and weight of public interests.[59] Where appropriate, the ALRC suggests some guidance on the relevant factors the court might or should consider.[60]

2.35 The ALRC has specifically addressed the desirability of precision and certainty in its recommendations, particularly in relation to the design of a statutory cause of action and in relation to reforming Australia's fragmented surveillance laws.[61]

Principle 7: Privacy laws should be coherent and consistent

2.36 Coherence in the law and consistency with other Australian laws or regulatory regimes should be an important guiding force in any new privacy protection at law. In making recommendations in this Report, the ALRC aims to promote uniformity or consistency in the law throughout Australian jurisdictions.

2.37 Laws that are unnecessarily complex, fragmented and inconsistent impose an unnecessary regulatory burden on business. They also harm privacy. The ALRC heard concerns about differences in privacy-related laws—such as surveillance device laws—between the various states and territories.[62] These differences can cause uncertainty and confusion, and make the law less effective.

2.38 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 and other businesses, which operate nationally, may be overly restricted if it is unclear when and where they might be breaching a law.[63]

2.39 The need for coherence and consistency also underlies the desirability of avoiding unnecessary overlap between legal regimes. Stakeholders said that any proposed remedial regime should not overlap or be inconsistent with the various regulatory schemes and statutory prohibitions that already affect them.[64] This was a particular concern given the amendments to the *Privacy Act 1988* (Cth) that came into force in March 2014.

2.40 However, regulation, the criminal law and the civil law can serve different purposes, even if they overlap in some ways. For example, a criminal law may aim to punish the perpetrator and deter similar conduct, while a civil cause of action may aim to give victims a remedy.

---

59 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*.

60 See, eg, Ch 8.

61 See Ch 14.

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

63 ASTRA, *Submission 47*; ABC, *Submission 46*.

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

2.41 Furthermore, although there are many regulatory regimes, criminal laws and civil obligations and remedies that help protect people from breaches or invasions of privacy, there are also a number of notable gaps in these laws. This Report aims to fill some of these gaps.

2.42 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,[65] 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

2.43 The law should provide a range of means to prevent, reduce or redress serious invasions of privacy. Recommendations in this Report aim to facilitate access to justice for individuals affected by serious invasions of privacy. For the Women's Legal Services NSW, access to justice means that

> it must be fair, simple, affordable and easy to understand and navigate. It must also have pathways for early intervention to prevent further disadvantage.[66]

2.44 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.[67] The law should make appropriate provision for people with disability or others who require assistance in obtaining access to justice.[68] The Terms of Reference for the ALRC's Inquiry into Equality, Capacity and Disability in Commonwealth Laws—being conducted at the same time as this Inquiry—refer to ensuring that Commonwealth laws and legal frameworks are responsive to the needs of people with disability and to advance, promote and respect their rights, in the area of access to justice and legal assistance program.[69]

2.45 The Productivity Commission has stated that a 'well functioning justice system':

> means delivering fair and equitable outcomes as efficiently as possible and resolving disputes early, expeditiously and at the most appropriate level. A justice system which effectively excludes a sizable portion of society from adequate redress risks considerable economic and social costs.[70]

---

65 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.

66 Women's Legal Services NSW, *Submission 57*.

67 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*.

68 Office of the Public Advocate (Queensland), *Submission 12*. Representative actions are discussed in Ch 10.

69 Australian Law Reform Commission, *Equality, Capacity and Disability in Commonwealth Laws*, Discussion Paper 81 (2014).

70 'Access to Justice Arrangements' (Draft Report, Productivity Commission, 2014) v.

2.46 In Chapter 16, the ALRC recommends that the Privacy Commissioner be empowered to hear complaints about serious invasions of privacy. This may be one way of increasing access to justice. Other recommendations also encourage, without compelling, people to pursue alternative dispute resolution mechanisms.[71]

Principle 9: Privacy protection is an issue of shared responsibility

2.47 Individuals must generally take some responsibility for the protection of their own privacy and the privacy of others. The exercise of personal responsibility should be encouraged, where possible. The ALRC considers that capable adults should be encouraged to take reasonable steps to use the privacy tools offered by service providers. Several stakeholders stressed the importance of personal responsibility.[72]

2.48 However, government, corporations and small businesses that process personal information also have a responsibility to provide individuals with the necessary tools to protect their own privacy. Personal responsibility can only be fully exercised when individuals are provided with the education and tools necessary to protect their privacy, and when the choices expressed by individuals are respected.[73]

2.49 Individual responsibility must therefore be balanced with the responsibility of organisations and service providers. These groups 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.

2.50 In some circumstances, individuals may not be empowered to exercise personal responsibility in a meaningful way. Professor Daniel Solove has written that, although privacy self-management is 'certainly a laudable and necessary component of any regulatory regime', it is being 'tasked with doing work beyond its capabilities'.[74]

2.51 The ALRC is asked to consider how the *law* may redress and reduce serious invasions of privacy. But the law is not a panacea, and education has an important role to play in reducing and preventing serious invasions of privacy.[75]

2.52 In the ALRC's view, governments and industry have a responsibility to provide adequate education and assistance, particularly for vulnerable members of the Australian community, such as people living with disabilities, children and some young people.

---

71 Several stakeholders supported voluntary alternative dispute resolution under the new privacy tort: 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*.

72 Australian Federal Police, *Submission 67*; Facebook, *Submission 65*; National E-Health Transition Authority, *Submission 8*.

73 Australian Privacy Foundation, *Submission 110*.

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

75 Australian Federal Police, *Submission 67*; Facebook, *Submission 65*; Google, *Submission 54*.

2.53 The OECD's 2013 *Privacy Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* highlighted the need for greater government investment in education about privacy awareness, particularly concerning online privacy protection. The Guidelines recognise that 'more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks'.[76]

2.54 Education about privacy risks and management may be particularly important for children and young persons.[77] Research suggests that the use of privacy settings on social media is higher among older Australians. For instance, sixteen to seventeen year olds are significantly more likely to have their Facebook profiles set to private—limiting access to their private information to individuals whose online 'friendship' they have accepted—compared to twelve to fifteen year olds.[78] This is affirmed by evidence suggesting some young people believe the internet to be a 'necessity of life' and that 'it is better to take a beating from all your classmates than to be isolated from the Internet'.[79]

2.55 This evidence may suggest the need for privacy awareness campaigns and other strategies targeted at younger Australians.

2.56 Drs Nicola Henry and Anastasia Powell underscored the importance of non-legal methods to reducing and redressing invasions of privacy which occur through the internet:

> Service providers of online communities and social media networks can and should be proactive in addressing these issues by providing mechanisms for users to report hateful and/or harassing content and can dedicate sufficient resources towards monitoring and removing such content. Clear community guidelines, terms of use on internet sites, and agreement between police and service providers may also be effective. Educational initiatives are crucial in fostering an ethical digital citizenship and can do much to educate people about the right to privacy.[80]

2.57 The overall balance of recommendations in this Report is informed by the principle that responsibility for protecting privacy must often be shared.

---

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

77 Facebook, *Submission 65*; National Children and Youth Law Centre, *Submission 61*.

78 Australian Communications and Media Authority Australian Government, 'Like, Post, Share—Short Report: Young Australians and Online Privacy' (May 2013).

79 Niels Baas, Menno de Jong and Constance Drossaert, 'Children's Perspectives on Cyberbullying: Insights Based on Participatory Research' (2013) 16 *Cyberpsychology, Behaviour and Social Networking* 248, 252.

80 N Henry and A Powell, *Submission 104*.

3. Overview of Current Law

Contents

Summary 41
Existing legislative privacy protection 42
- Information privacy 42
- Health information privacy 44
- Communications privacy 44
- Surveillance laws and laws affecting photography 45
- Harassment and stalking offences 46
- Industry codes and guidelines 47

Existing common law causes of action 47
- Physical intrusions 48
- Surveillance from outside a property 48
- Intrusions into airspace 49
- Defamatory publications 50
- Disclosures of confidential information 50
- Unauthorised photography 51

Filling the gaps in existing law 51
A common law action for breach of privacy in Australia? 53

Summary

3.1 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 the 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.

3.3 An understanding of these gaps and deficiencies is important background to the recommendations in this Report.

3.4 This chapter concludes with an outline of recent case law in which the possibility of a new common law cause of action for invasion of privacy has been raised.

Existing legislative privacy protection

Information privacy

3.5 The *Privacy Act 1988* (Cth) 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]

3.6 The *Privacy Act* provides 13 'Australian Privacy Principles' (APPs) that regulate the 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]

3.7 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.

3.8 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]

3.9 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 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 5–3.

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

4 'APP entity' is defined in s 6(1) of the *Privacy Act*. 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 s 6E of the *Privacy Act*.

6 Ibid 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]

3.10 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]

3.11 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]

3.12 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;[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]

3.13 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] These laws provide various mechanisms for individuals to make complaints and seek redress. The *Privacy and Personal Information Protection Act 1998* (NSW), for example, provides powers to the NSW Privacy Commissioner that

---

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). See Ch 16 on the potential for this path to be an important source of access to the courts if a wider complaints mechanism is introduced into the Act.
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); *Information Privacy Act 2014* (ACT); *Information Act* (NT).

are primarily conciliatory,[17] while the *Information Privacy Act 2009* (Qld) provides for the referral of complaints to Queensland's Civil and Administrative Tribunal (QCAT),[18] which may order, among other things, that the complainant is entitled to up to $100,000 in compensation.[19]

3.14 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 organisations that are exempt from the application of any of these Acts and whose activities may have an impact on individual privacy. These may include, for example, many small businesses.[20]

3.15 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

3.16 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.[21] Separate Commonwealth Acts protect healthcare identifiers[22] and electronic health records.[23]

3.17 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.[24]

Communications privacy

3.18 The *Telecommunications Act 1997* (Cth) prohibits the disclosure of certain information by telecommunications providers.[25] Contravention of these prohibitions is an offence punishable by up to two years imprisonment.[26]

---

17 *Privacy and Personal Information Protection Act 1998* (NSW) s 49. The Act also provides for an individual to make a complaint to the agency in question, and to apply to the Administrative Appeals Tribunal for a review of an agency's decision. The Tribunal may make a variety of orders, including an order that the agency pay the individual compensation of up to $40,000: *Privacy and Personal Information Protection Act 1998* (NSW) ss 53–55.

18 *Information Privacy Act 2009* (Qld) s 176(1).

19 Ibid s 178(a)(v).

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

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

22 *Healthcare Identifiers Act 2010* (Cth).

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

24 *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).

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

26 Ibid s 276(3).

3.19 There are a number of exceptions, for example, for disclosures to the Australian Security Intelligence Organisation 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,[27] but this does not permit the disclosure of the contents or substance of a communication.[28] An authorised officer must consider the privacy of any person before making an authorisation.[29]

3.20 The TIA Act prohibits the unauthorised access of communications, subject to various exceptions,[30] unless a warrant is obtained.[31] Those who issue warrants must consider, among other things, the privacy of persons affected by the access.[32]

3.21 The TIA Act also prohibits the unauthorised interception of communications over a telecommunications system, again, subject to various exceptions,[33] unless a warrant is obtained.[34] Those who issue an interception warrant must consider, among other things, the privacy of persons affected by the interception.[35]

Surveillance laws and laws affecting photography

3.22 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.[36] The surveillance device laws also place restrictions on communicating information obtained through the use of a surveillance device.

3.23 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.[37]

3.24 Different state and territory workplace surveillance legislation prohibits employers monitoring their employees at work through covert surveillance methods,

---

27 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 171–182.
28 Ibid s 172. A disclosure under these provisions is therefore limited to communications data ('metadata').
29 Ibid s 180F.
30 Ibid s 108.
31 Ibid ss 110–132.
32 Ibid s 116(2).
33 Ibid s 7.
34 Ibid ss 9–18, 34–61A.
35 Ibid ss 46(2), 46A(2).
36 *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).
37 See Ch 13.

such as the use of CCTV cameras or computer, internet and email surveillance.[38] Once again, there are inconsistencies between these laws, and such laws only exist in three jurisdictions—NSW, Victoria and the ACT.

3.25 Criminal laws in some—but not all—jurisdictions provide for offences relating to photography being used for indecent purposes[39] or indecent filming without consent.[40] Criminal laws also provide protection against indecent photography of children in private and public places.[41] 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.

3.26 At the Commonwealth level, the operation of the *Privacy Act* is restricted to the actions of government agencies and big business, and does not cover 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'.[42] This may provide scope to regulate the actions of photographers who take unauthorised photographs of individuals.[43]

Harassment and stalking offences

3.27 State and territory laws criminalising harassment and stalking vary considerably by jurisdiction. Legislation in Queensland and Victoria expressly prohibits 'cyber-harassment' committed through 'electronic messages'[44] or by 'otherwise contacting the victim'.[45]

3.28 The *Criminal Code Act 1995* (Cth) 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'[46] and 'using a carriage service to make a threat'.[47]

---

38 *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic); *Workplace Privacy Act 2011* (ACT).

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

40 *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.

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

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

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

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

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

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

47 Ibid s 474.15.

3.29 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.[48]

Industry codes and guidelines

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

3.31 Commercial television and radio broadcasters are subject to a self-regulatory scheme under the *Broadcasting Services Act 1992* (Cth). Commercial broadcasting industry codes of practice include provisions relating to the protection of privacy.[49] 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.[50] The Australian Communications and Media Authority (the ACMA) has oversight of each of these codes of practice, however the ACMA has limited powers to provide redress to individuals when a code is breached.

3.32 The Australian Press Council oversees the compliance of its members with its *Charter of Press Freedom* (2003) and *Statement of Privacy Principles* (2011). It does not provide a mechanism for individuals to obtain monetary redress.

3.33 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

3.34 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.[51] These causes of action protect against physical intrusions upon a person, surveillance of a person, and against unauthorised disclosure of private information.

---

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

49 Commercial Television Industry Code of Practice 2010 cl 4.3.5; Commercial Radio Codes of Practice and Guidelines 2011 cl 2.1(d).

50 ABC Code of Practice 2011 cl 6.1; SBS Codes of Practice 2014 cl 1.9.

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

Physical intrusions

3.35 Trespass to the person and trespass to land provide some protection against unauthorised interference with a person's body or intrusions into property.[52] 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 plaintiff to establish any recognised form of damage such as personal injury, psychiatric illness, property damage or economic loss.

3.36 'General' damages, sometimes substantial, are awarded to compensate the plaintiff for the wrong that has occurred, and for any actual damage sustained, or by way of solace or vindication of his or her rights.[53] Aggravated damages may be awarded where there is a special humiliation of the plaintiff 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 plaintiff's rights.[54] Plaintiffs may seek injunctions to restrain the broadcast of video material recorded without authorisation while a defendant was trespassing on land,[55] although damages have been deemed an adequate remedy in cases involving commercial enterprises.[56]

3.37 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.

3.38 Trespass to land also has strict requirements as to the title over the land that the plaintiff 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[57] or the occupation of a hospital bed or room,[58] 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 plaintiff 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

3.39 A person may be liable in the tort of nuisance for an unreasonable interference with an occupier's use and enjoyment of their land.[59] For example, a person may be found liable in nuisance for keeping the occupier under surveillance or by positioning

---

52 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.
53 *Plenty v Dillon* (1991) 171 CLR 635, 654–655 (Gaudron and McHugh JJ).
54 *XI Petroleum (NSW) Pty Ltd v Caltex Oil (Australia) Pty Ltd* (1985) 155 CLR 448.
55 *Emcorp Pty Ltd v Australian Broadcasting Corporation* [1988] 2 Qd R 169.
56 *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457; *Brigthen Pty Ltd v Nine Network Australia Pty Ltd* [2009] NSWCA 319.
57 *Douglas v Hello! Ltd* [2005] EWCA Civ 595 (18 May 2005).
58 *Kaye v Robertson* [1991] FSR 62.
59 Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) ch 14.

cameras or lights in situations where they interfere with, record or 'snoop' on the occupier's activities.[60] As in trespass, 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.[61]

Intrusions into airspace

3.40 Intrusions into airspace may amount to trespass to land if the intrusion is at a height that is potentially necessary for the ordinary use and enjoyment of the occupier.[62] Exceptions apply in the case of aircraft merely flying 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) 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.[63]

3.41 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, which nevertheless come with the definition of aircraft.

3.42 It is a question of fact in the circumstances as to whether or not a trespass has occurred according to common law principles. This would depend on whether the potential use and enjoyment of the land and airspace by the occupier has been interfered with from within the relevant height limit of the occupier's interests.[64] If the interference was from outside the occupier's airspace, the circumstances could amount to a nuisance at common law.

3.43 In the case of aircraft, whether or not a trespass has occurred would also depend on whether or not the height of the intrusion is reasonable in all of the circumstances.[65] Mere compliance with Air Navigation Regulations, which are aimed at safety issues,[66] 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.[67] Aerial photography, recording and surveillance carried out from a plane or helicopter

---

60 *Raciti v Hughes* (1995) 7 BPR 14 837. The plaintiffs successfully obtained an injunction to prevent the use of motion-triggered lights and surveillance cameras aimed at their backyard.

61 *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.

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

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

64 *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.

65 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.

66 Civil Aviation Safety Authority, *Submission 2*.

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

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.

3.44 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.[68]

Defamatory publications

3.45 The tort of defamation provides redress for a person whose reputation is damaged by a publication to a third party. Until the enactment of the Uniform Defamation Laws in 2005 in Australian states and territories,[69] defamation law provided considerable indirect[70] 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.[71] However, the truth of a defamatory statement is now a complete defence, so that defamation actions provide much more limited protection of privacy.[72]

Disclosures of confidential information

3.46 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.

3.47 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,[73] although they might refuse relief where the parties had already been very public about their relationship.

---

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

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

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

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

72 Sappideen and Vines, above n 51, ch 25.

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

3.48 It is now well accepted in the United Kingdom[74] (UK) and Australia[75] 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, although there is still some uncertainty in Australia as to what compensation is available in an equitable action for breach of confidence.[76]

Unauthorised photography

3.49 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 their consent.[77] There is also no prohibition on taking photographs of private property from public land, unless the conduct amounts to stalking or the intent is to 'peep or pry' on an individual.[78] 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.[79]

Filling the gaps in existing law

3.50 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.[80] A statutory cause of action for serious invasions of privacy,[81] or a statutory tort for harassment,[82] 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.[83] The ALRC recommends that a tort for serious invasions of privacy should be actionable *per se*, therefore allowing for the recovery of damages for emotional distress.[84]

---

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

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

76 See Ch 13.

77 '[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).

78 See, eg, *Crimes Act 1900* (NSW) s 547C.

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

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

81 See Chs 4–12.

82 See Ch 15.

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

84 See Ch 8.

- 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. This uncertainty should be removed.[85]
- 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.[86] The Discussion Paper included a proposal that courts be required to give particular consideration to freedom of expression and matters of public interest when considering such an injunction on the basis of common law actions.[87] The ALRC considers that it may be premature to proceed with this proposal unless and until there is further development of the common law.[88]
- Legislation dealing with surveillance and with workplace surveillance is not uniform throughout Australia, and is outdated in some states. The ALRC recommends that these surveillance device laws should be made replaced by a Commonwealth Act.[89]
- There is no tort or civil action for harassment, nor is there sufficient deterrence against 'cyber-harassment' in Australian law, compared with overseas jurisdictions.[90] The ALRC recommends civil remedies and criminal penalties for harassment if a statutory cause of action for serious invasion of privacy is not enacted.[91]
- 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.[92] This limitation would be addressed by the statutory cause of action for serious invasions of privacy. In addition, ALRC recommendations for the replacement of state and territory

85 See Ch 13.

86 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.

87 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) Prop 12–2.

88 See Ch 13.

89 See Ch 14.

90 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), c 2 criminalises cyber-bullying.

91 See Ch 15 and in particular Rec 15–1.

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

surveillance devices laws would technology-neutral legislation would allow for the regulation of new means of surveillance.[93]

- 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, by way of complaints made to the Australian Information Commissioner. While of central importance, this legislation by no means covers the field of invasions of privacy. The Act does not generally apply to intrusions into personal privacy or to the behaviour of individuals or media entities,[94] and does not generally apply to businesses with an annual turnover of less than $3 million.[95]
- There is no regulatory avenue for monetary redress for complaints about invasions of privacy by media or communications entities.[96]

3.51 Some of the gaps identified above are more properly dealt with by existing regulatory bodies. Some concerns have been the subject of recent, carefully considered enactments—for example, the recent amendments to the *Privacy Act* made by the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), many of which came into effect only in March 2014, three months before the completion of this Inquiry.

3.52 Further, in many instances a targeted review of existing legislation which is the subject of community debate is more appropriate. For example, the privacy protections under the *Telecommunications Act* and the TIA Act were the subject of a 2013 Parliamentary Inquiry.[97] At the time of writing, a further Parliamentary Inquiry is ongoing.[98] The ALRC therefore does not consider these provisions in this Report.

A common law action for breach of privacy in Australia?

3.53 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.[99] A tort of invasion of privacy has been recognised by two lower court decisions: *Grosse v Purvis* in the District Court of Queensland[100] and *Doe v Australian Broadcasting*

93 See Ch 14.

94 A proposal to extend the Commissioner's powers to investigate complaints about serious invasions of privacy is considered in Ch 16. This extension would make use of the Commissioner's existing powers, including powers to make non-binding declarations. This power could also allow the Commissioner to investigate complaints about serious invasions of privacy by the media.

95 The small business exemption in the *Privacy Act* is discussed in Ch 16.

96 See above on the Australian Press Council. The ALRC has not proceeded with a proposal for the ACMA to be given equivalent, limited powers to the OAIC to redress complaints of serious unjustified invasions of privacy.

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

98 Legal and Constitutional Affairs References Committee, *Comprehensive Revision of Telecommunications (Interception and Access) Act 1979* (referred by Senate on 12 December 2013; reporting date 27 August 2014).

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

100 *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.

Corporation[101] in the County Court of Victoria. However, both cases were settled before appeals by the respective defendants were heard.

3.54 No Australian appellate court has confirmed the existence of this tort, and the judgments of several courts suggest that the common law is unlikely to recognise the tort in the foreseeable future:

- 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;[102]
- 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';[103]
- 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';[104] and
- in *Giller v Procopets*,[105] 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.

3.55 In other cases, the existence of the tort at common law has been left open:

- 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 '[t]hese 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;[106]
- in *Saad v Chubb Security Australia Pty Ltd*, Hall refused to strike out a claim for breach of confidence, holding that it was not 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';[107]
- in *Gee v Burger*, McLaughlin AsJ considered the matter 'arguable';[108]
- 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';[109] and

---

101 *Doe v Australian Broadcasting Corporation* [2007] VCC 281 (2007).
102 *Kalaba v Commonwealth of Australia* [2004] FCA 763 (8 June 2004) [6].
103 *Chan v Sellwood; Chan v Calvert* [2009] NSWSC 1335 (9 December 2009) [34].
104 *Sands v State of South Australia* [2013] SASC 44 (5 April 2013) [614].
105 *Giller v Procopets* (2008) 24 VR 1.
106 *Maynes v Casey* [2011] NSWCA 156 (14 June 2011) [35].
107 *Saad v Chubb Security Australia Pty Ltd* [2012] NSWSC 1183 [183].
108 *Gee v Burger* [2009] NSWSC 149 (13 March 2009) [53].

- 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'.[110]

3.56 The cases suggest that the future development of the common law is, at best, uncertain. Moreover, any significant development of the common law would require litigants with the resources and determination both to initiate proceedings and to take those proceedings through the appeals process. In *Goodwin v News Group Newspapers* —a case involving a privacy claim against a media defendant in the UK—Tugendhat J noted that

> it is essential that the parties to litigation put their evidence and submissions before the court. It is by weighing up arguments and counter arguments that judges are best able to interpret the law. … To the extent that media defendants choose not to submit evidence and argument to the courts, judges will find it difficult to develop the law of privacy to meet the needs of society.[111]

3.57 There are indications that litigants may prefer to rely on the limited remedies of well-established causes of action, rather than risk the prolonging of proceedings or appeals on uncertain points of law or novel arguments. This is particularly so if the monetary compensation for any new cause of action is not likely to be high.

3.58 However, the dependence on parties to bring their case or assert their defence in court is an inherent feature of the system underlying the development of the common law.[112] It is unlikely that Australian law on privacy will stand still indefinitely, even if its precise development cannot yet be predicted.

109 *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.

110 *Doe v Yahoo!7 Pty Ltd* [2013] QDC 181 (9 August 2013) [310]–[311].

111 *Goodwin v NGN Ltd* [2011] EWHC 1437 (QB) [145] (Tugendhat J).

112 See Ch 1.

Part 2

4. A New Tort in a New Commonwealth Act

Contents

Summary 59
A new stand-alone Commonwealth Act 59
Constitutional issues 62
Head of power 62
Constitutional limits 66
An action in tort 67
Abolition of common law actions 72

Summary

4.1 This chapter sets out the ALRC's recommendation that a statutory cause of action for serious invasions of privacy should be contained in a new, stand-alone Commonwealth Act.

4.2 Locating the new action in a Commonwealth Act would ensure uniformity and consistency in the operation of the cause of action throughout Australia. Uniformity of law across Australia was consistently identified by stakeholders as important, particularly to avoid the unnecessary costs to business that arise from inconsistent legal regimes across the country.

4.3 In the ALRC's view, 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. Further, the *Privacy Act* has a number of exemptions which would not apply to the new action.

4.4 The ALRC recommends that a statutory cause of action for serious invasions of privacy should be a tort to provide 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.

A new stand-alone Commonwealth Act

Recommendation 4–1 If a statutory cause of action for serious invasion of privacy is to be enacted, it should be enacted by the Commonwealth, in a Commonwealth Act (the Act).

4.5 This recommendation is about the location of a statutory cause of action in Australian law. There are two aspects to this recommendation: that the legislation should be enacted by the Commonwealth rather than by the states and territories; and that the statutory cause of action should preferably be located in a stand-alone Act, rather than the *Privacy Act*.

4.6 First, the ALRC considers that if a statutory cause of action is introduced, it should be in Commonwealth legislation, as this is the best way to ensure the action is available and consistent throughout Australia. Many stakeholders emphasised the need for and value of uniformity and consistency of law across Australia.[1]

4.7 The Western Australian Attorney-General submitted that co-operative Commonwealth and state legislation would be preferable.[2] However, it is demonstrably difficult to achieve consistency across state and territory legislation,[3] and even where this has been achieved on certain legal issues, it has taken a very long time.[4] Inconsistent statutory provisions in state and territory legislation would be highly confusing, and increase fragmentation and unnecessary complexity in the law. Complexity would result in 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 substantially increases 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.

4.8 On the second aspect of the recommendation, the ALRC considers that the better course is for the cause of action to be in a stand-alone Act to avoid confusion and to enhance clarity.[5] The court-ordered remedial regime that would follow invasions of privacy under the statutory cause of action would be distinct from the regulatory regime which is the essence of the *Privacy Act.*

4.9 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'

---

1 Public Interest Advocacy Centre, *Submission 105*; South Australian Law Reform Institute, *Submission 87*; Australian Pork Ltd, *Submission 83*; Office of the Australian Information Commissioner, *Submission 66*. Australian Pork Ltd also noted that enacting a Commonwealth Act would be quicker than the time frame needed for uniform state and territory legislation.

2 Office of the Western Australian Attorney-General, *Submission 25*.

3 This is illustrated by the continuing variation in surveillance devices legislation discussed in Ch 14, but also in other regimes such as civil liability legislation.

4 See, eg, the Uniform Defamation Laws, finally introduced in 2005 after 150 years of inconsistency, and decades of discussion on reform. David Rolph, 'A Critique of the National, Uniform Defamation Laws' (2008) 16 *Torts Law Journal* 207.

5 In 2008, the ALRC also expressed this view, stating 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': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [74.195].

regulation). The statutory cause of action would relate not only to the privacy of information but also to other types of privacy, such as territorial, communications and bodily privacy.

4.10 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.[6] However, breaches of the requirements of the *Privacy Act* generally lead to regulatory responses by the Office of the Australian Information Commissioner (OAIC) including, from March 2014, the possible imposition of significant civil penalties on the relevant entity.[7] By contrast, an invasion of privacy that is actionable under the Act would lead only to a range of civil remedies sought by and for the benefit of the plaintiff.

4.11 Importantly, the *Privacy Act* is limited in its application to certain entities across Australia. It does not apply to most individuals,[8] or to state agencies. It also includes a number of exemptions, such as for small businesses (defined as having an annual turnover of less than $3 million) and media and other activities.[9] The ALRC recommends that there be no limitations or exemptions under the statutory cause of action. Subject to jurisdictional limitations, any justification in the public interest or defences including lawful authority,[10] the new statutory cause of action would apply to any person or entity that invades the privacy of a person in the manner and circumstances set out in the Act.

4.12 A number of stakeholders considered that the cause of action, if enacted, should be contained in the *Privacy Act*.[11] Dr Normann Witzleb submitted that the cause of action is consistent with the objects of the *Privacy Act*, would make the name of that Act more appropriate, and would involve the Privacy Commissioner being given additional powers.[12] The Media and Communications Committee of the Law Council of Australia submitted that, if it were enacted, a statutory cause of action should be in the *Privacy Act* and subject to the existing media exemptions.[13]

4.13 On balance, and particularly because it recommends that the statutory cause of action should *not* include the exemptions in the *Privacy Act*, the ALRC considers that it

---

6 The existing complaints mechanism is discussed in Ch 15.

7 These responses are outlined in Ch 3.

8 As noted in Ch 3, the *Privacy Act* does apply to some individuals, including individuals who operate certain types of businesses and businesses that trade in personal information: see *Privacy Act 1988* (Cth) ss 6C–6EA. Section 16 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.

9 Ibid ss 6C(1), 6D (small businesses); s 7B(4) (journalistic acts); and s 7C (political acts).

10 The defence of lawful authority provides a significant exemption to a wide range of government and other agencies. See Ch 11.

11 N Witzleb, *Submission 116*; Australian Bankers' Association, Submission No 72 to DPM&C Issues Paper, 2011.

12 N Witzleb, *Submission 116*. See, also, Australian Bankers' Association, Submission No 72 to DPM&C Issues Paper, 2011.

13 Media and Communications Committee of the Law Council of Australia, *Submission 124*.

would be less confusing if the new cause of action were located in a new stand-alone Commonwealth Act. It would be appropriate for this Act to be called the *Serious Invasions of Privacy Act*.

4.14 If, however, an enhanced and broader model of complaints to the Australian Privacy Commissioner were to be introduced, as proposed by the OAIC, to provide complainants with an alternative to court proceedings in respect of invasions of privacy in general, there would be a stronger case for including the statutory cause of action in the *Privacy Act*.[14] The OAIC's proposal for a complaints model is discussed in Chapter 16.

Constitutional issues

Head of power

4.15 This section examines the scope of the Commonwealth's power under the *Australian Constitution* to legislate for the new tort. This issue was discussed in the ALRC's report, *For Your Information: Privacy Law and Practice* (2008).[15] The constitutional aspects of the ALRC's recommendations with regard to surveillance and harassment legislation are discussed in chapters 14 and 15 respectively.

4.16 The Commonwealth has the power to make laws with respect to 'external affairs'.[16] This power enables the Commonwealth to give effect to its international obligations under a bona fide treaty.[17] 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'.[18] This is a key issue in considering the constitutionality of a Commonwealth statute providing a cause of action. The ALRC noted in 2008 that the *Privacy Act* was enacted on the basis of the external affairs power and other powers.[19]

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

---

14 'If a new cause of action is actionable only in the courts, further consideration should be given as to whether the provisions are included in either the Privacy Act or in separate Commonwealth legislation. On the one hand, there is benefit in having all federal privacy regulation within the same piece of legislation. On the other hand, the Privacy Act largely pertains to the OAIC's functions, so provisions unrelated to the OAIC may be better placed in other legislation': Office of the Australian Information Commissioner, *Submission 66*.

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

16 *Australian Constitution* s 51(xxix).

17 *Commonwealth v Tasmania* (1983) 158 CLR 1, 130–131, 172, 232, 259 (The Tasmanian Dam case). See, also, *Richardson v Forestry Commission* (1988) 164 CLR 261, 289; 303; *Castlemaine Tooheys v SA* (1990) 169 CLR 436, 473; *Victoria v Commonwealth* (1996) 187 CLR 416 at 487. The Commonwealth is not required to implement all provisions of a treaty.

18 *Victoria v Commonwealth* (1996) 187 CLR 416, 487 (Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ).

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) 195–196, referring to the Preamble. See now *Privacy Act 1988* (Cth) s 2A: 'The objects of this Act are (h) to implement Australia's international obligation in relation to privacy.'

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

4.18 The ICCPR was ratified by Australia subject to a number of reservations and declarations which included, in relation to art 17, the right to 'enact and administer laws which, insofar as they authorise action which impinges on a person's privacy, family, home or correspondence, are necessary in a democratic country in the interests of national security, public safety, the economic well-being of the country, the protection of public health or morals, or the protection of the rights and freedoms of others'.[20] Australia withdrew this reservation to art 17 on 6 November 1984.

4.19 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 invasions of privacy would be valid on the basis that the law would be reasonably capable of being considered appropriate and adapted to fulfilling Australia's obligations under art 17 of the ICCPR.

4.20 To reflect art 17, the new tort would need to be seen as a measure aimed at prohibiting or regulating certain conduct in order to protect privacy.

4.21 Article 17 is intended to be a general protection against arbitrary or unlawful interference with privacy; it is not intended merely to restrict the actions of governments. The Human Rights Committee, which is an independent body established to supervise the application of the ICCPR,[21] in its General Comment 16 on art 17, states:

> In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons.
>
> …
>
> States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.[22]

---

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

21 Ibid art 28.

22 Human Rights Committee, *General Comment No 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)*, 35th sess, UN Doc A/43/40 (28 September 1988) [1], [9]. The views of the Human Rights Committee, while not binding, represent a strongly persuasive view of what the international obligation entails. The High Court has been prepared to have regard to a range of international law sources in interpreting international obligations, see, eg, *R v Tang* (2008) 237 CLR 1.

4.22 'Arbitrary interference' means interferences that are not reasonable in the particular circumstances. General Comment 16 says expressly:

> The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[23]

4.23 In its *Toonen* decision, the Human Rights Committee also said:

> The Committee interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.[24]

4.24 The High Court grants some latitude to Parliament in selecting the means by which to give effect to a treaty obligation.[25]

4.25 It has been suggested that a treaty setting out a 'broad objective with little precise content and permitting widely divergent policies by parties' may not be sufficiently specific to support legislation.[26] However, the High Court has recognised that international obligations need not be defined with the precision required under domestic law, and that 'absence of precision does not, however, mean any absence of international obligation'.[27] 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, so that there is not a problem of insufficient specificity.

4.26 The ALRC considers that the enactment of a statutory cause of action for serious invasion of privacy carries the provisions of art 17(2) into effect and satisfies the requirement of proportionality. The creation of the action is likely to act as a disincentive to engage in invasions of privacy in Australia. Conferring a private right to redress will have the effect of protecting persons from interferences with their privacy. Further, in addition to according individuals the 'protection of law' as required by art 17(2), a statutory cause of action could be said to further the fulfilment of Australia's obligation to provide an effective remedy to violations of art 17 as required by art 2(3) of the ICCPR.

4.27 The limited interests protected by the cause of action are generally accepted as falling within the notion of 'privacy'. To aid the courts in interpreting the statutory cause of action, it could be made clear in the Act or extrinsic material (such as the

---

23 *R v Tang* (2008) 237 CLR 1, [4].

24 Human Rights Committee, Communication No. 488/1992, UN Doc CCPR/C/50/D/488/1992 (4 April 1994).

25 Leslie Zines, *The High Court and the Constitution* (Butterworths, 4th ed, 1997) 288; Sir Anthony Mason, 'The Influence of International Law and Transnational Law on Australian Municipal Law' (1996) 7 *Public Law Review* 20, 24. See, also, *Victoria v Commonwealth* (1996) 187 CLR 416, 486–487; *Richardson v Forestry Commission* (1988) 164 CLR 261, 289, 296.

26 *Victoria v Commonwealth* (1996) 187 CLR 416, 486.

27 *Commonwealth v Tasmania* (1983) 158 CLR 1, 242; *Victoria v Commonwealth* (1996) 187 CLR 416, 486.

Explanatory Memorandum) that Parliament did not intend that the cause of action would extend beyond what is encompassed in the notion of 'privacy' in art 17.

4.28 In its 2008 report, the ALRC canvassed other heads of power as a basis for legislating on privacy, which may also support aspects of the statutory cause of action.[28] One of these was the Commonwealth's power to legislate with respect to 'postal, telegraphic, telephonic and other like services'.[29] The technology-neutral phrase 'other like services' demonstrates that the possibility of developments in technology was contemplated by drafters when framing s 51(v).[30] Radio and television broadcasting have been held to be within the Commonwealth's power under s 51(v).[31] Although the Commonwealth's power to regulate the internet under this head of power is yet to be considered by the High Court, it does not seem controversial that it would be a 'like service'.[32]

4.29 The ALRC notes that a number of other powers could be relied upon to provide partial support for Commonwealth legislation enacting a statutory cause of action, but they would not in total provide the Commonwealth with the full support that the external affairs power would provide. The legislation enacting the statutory cause of action could, however, include a 'reading down' provision, invoking the communications power and the following additional heads of power to ensure that the legislation is as robust as possible from a constitutional perspective:

- s 51(xx) of the Constitution, which gives the Parliament the power to make laws with respect to 'foreign corporations, and trading or financial corporations formed within the limits of the Commonwealth';
- s 122 which confers near plenary power on the Commonwealth to legislate in respect of the Territories;
- ss 51(xiii) and (xiv), the banking and insurance powers, which would enable the Commonwealth to legislate to regulate relevant conduct of persons engaging in the business of banking or insurance (provided this was not state insurance or state banking carried on within the limits of a state);
- s 51(i), the interstate and overseas trade and commerce power, which would enable the Commonwealth to legislate with respect to relevant conduct engaged in in the course of interstate or overseas trade or commerce;

---

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) 196; *Australian Constitution* s 51(i), (v), (xiii), (xiv), (xx).

29 *Australian Constitution* s 51(v).

30 *Grain Pool of Western Australia v Commonwealth* (2000) 202 CLR 479, 493.

31 *R v Brislan; Ex parte Williams* (1935) 64 CLR 262; *Jones v Commonwealth (No 2)* [1965] HCA 6 (3 February 1965).

32 Helen Roberts, 'Can the Internet Be Regulated?' (Research Paper No 35, Parliamentary Library, Parliament of Australia, 1996) 25.

- the 'geographically external' aspect of the external affairs power in s 51(xxix), which would permit the Commonwealth to legislate to regulate relevant conduct occurring outside Australia (eg the electronic surveillance of a person in Australia by a person outside of Australia); and
- s 51(xxxix), the express incidental power, which would enable the Commonwealth to regulate its own conduct and the conduct of bodies established by Commonwealth legislation.

4.30 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.[33]

Constitutional limits

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

Implied freedom of political communication

4.32 The legislative power of the Commonwealth is subject to the implied freedom of political communication,[34] although the precise scope of the communications protected is still a matter of some uncertainty. In assessing whether a law infringes the freedom, there are two questions.

4.33 The first question is, does the law effectively burden freedom of communication about government or political matters in its terms, operation or effect?

4.34 The second question is, 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?[35]

4.35 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'. This test has been affirmed in a number of recent decisions of the High Court.[36]

---

33 *Australian Constitution* s 109.

34 *Australian Capital Television v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *APLA Ltd v Legal Services Commissioner (NSW)* (2005) 224 CLR 322; *Unions NSW v State of New South Wales* (2013) 88 ALJR 227.

35 *Wotton v Queensland* (2012) 246 CLR 1; *Monis v The Queen* (2013) 87 ALJR 340; *Attorney-General (South Australia) v Corporation of the City of Adelaide* (2013) 249 CLR 1; *Unions NSW v State of New South Wales* (2013) 88 ALJR 227.

36 *Wotton v Queensland* (2012) 246 CLR 1; *Monis v The Queen* (2013) 87 ALJR 340; *Attorney-General for South Australia v Corporation of the City of Adelaide* [2013] HCA 3; *Unions NSW v State of New South Wales* (2013) 88 ALJR 227.

4.36 The ALRC considers that the recommended statutory cause of action would not infringe the implied freedom of political communication. The recommended cause of action requires that the court be satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest, and includes a number of relevant defences such as absolute privilege. It is suggested that freedom of expression be specified as including the freedom to discuss political 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.

4.37 However, it may be prudent to include a provision expressly stating that the Act does not apply to the extent (if any) that it infringes the implied freedom of political communication.[37]

Impact on states

4.38 The ALRC's 2008 report discussed the *Melbourne Corporation* principle, as an implied limitation on the Commonwealth's power to legislate. In 2012, 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.[38]

4.39 The immunity applies not only to state governments but also to state agencies, including state corporations, to the extent that they are carrying out the functions of the state.[39]

4.40 The ALRC considers that a statutory cause of action, while imposing a burden on state governments or agencies, would not curtail the states' capacity to function as governments. This is particularly so in view of the defence of lawful authority, which will provide government agencies including law enforcement agencies with protection from liability for serious invasions of privacy where that conduct was consistent with their statutory powers. The Act would not place any greater burden on a state (or states) than on the Commonwealth itself.[40]

An action in tort

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

---

37 The use of constitutional terms in this way has sometimes been criticised, but was recently upheld in *Wurridjal v Commonwealth* (2008) 237 CLR 309.

38 *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.

39 *Queensland Electricity Commission v Commonwealth* (1985) 159 CLR 192, 218.

40 *Austin v Commonwealth* (2003) 215 CLR 185; *Clarke v Commissioner of Taxation* (2009) 240 CLR 272.

4.41 There are a number of reasons for the ALRC's recommendation that the new cause of action should be specifically described as an action in tort.

4.42 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 purpose of determining whether other consequences follow at common law or under other statutes.[41] This would also be the case if a new statutory cause of action were enacted.[42] 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.[43] It may be relevant to decide whether an employer is vicariously liable to the plaintiff, 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.[44]
- 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.[45] Statutory contribution rights may apply only to 'tortfeasors'.[46]

---

41 *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].

42 The Australian Bankers' Association was the only stakeholder who raised concerns with this proposal, citing concerns about overlapping causes of action: Australian Bankers' Association, *Submission 84*. The ALRC notes, however, that it is commonplace for a person to have more than one cause of action and the courts are alive to the risk of double compensation. Doctrines such as issue estoppel and *Anshun* estoppel prevent undesirable duplication of litigation. Several stakeholders, including PIAC, agreed with the proposal but most did not comment: Public Interest Advocacy Centre, *Submission 105*.

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

44 *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. Professor Dan Svanntesson submitted that the ALRC in its Discussion Paper, while correctly stating the law, understated the complexity of the application of private international rules which 'will be far from a mechanical task even when the action is classed as a tort' and that it would be better to clarify the application of private international law rules to specific types of privacy violation that may attract liability under the tort, rather than leaving these matters in limbo: D Svantesson, *Submission 70*. However, given the wide range of possible factual situations, the ALRC doubts that such a task is feasible for any legislator and in any event such an attempt may quickly become outdated by changes in technology. Further, leaving the application of the general rules to the courts is more likely to lead to consistency when there are different causes of action arising out of the same conduct.

45 *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.

46 See, eg, *Law Reform (Miscellaneous Provisions) Act 1946* (NSW) s 5.

4.43 Describing the action as a tort action will therefore 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.[47]

4.44 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 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 to say that 'this definition is far from informative'.[48] Torts may be created by common law or statute.[49]

4.45 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 plaintiff, 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.

4.46 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 Act. This will enhance the coherence and consistency of the law.

4.47 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'.[50] The New Zealand courts have recognised new causes of action in

---

47 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 an employer is vicariously liable for the acts or the torts of an employee.

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

49 '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': Keith Stanton et al, *Statutory Torts* (Sweet & Maxwell, 2003) 6.

50 *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).

tort to protect privacy.[51] While 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), 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'.[52] While Australian courts may not be prepared to take the same leap in classification as may have occurred in the United Kingdom, the legislature is not so constrained.

4.48 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* and the *Broadcasting Services Act 1992* (Cth).

4.49 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.[53]

4.50 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.

4.51 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.[54] In the ALRC's view this point

---

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

52 *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] 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.

53 *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 v Bestnet Europe Ltd* [2013] 1 WLR 1556; *AMI Australia Holdings Pty Ltd v John Fairfax Publications Pty Ltd* [2010] NSWSC 1395.

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

seems to overlook or downplay the balancing that is required in some existing tort actions, such as in private nuisance, in which courts balance the interests of the plaintiff with those of the defendant in their respective use of their land.[55]

4.52 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.[56] The Victorian Law Reform Commission (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'.[57] Examples given were rules as to fault, damage, remedies and vicarious liability.

4.53 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.[58] 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 plaintiffs 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.[59]

4.54 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.[60] The ALRC considers that strict liability, or negligence based liability, would be oppressive or undesirable.[61] 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 recommends the integration of the

---

55 See Ch 9.

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

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

58 Free TV, *Submission 55*; The Newspaper Works, *Submission 50*; ASTRA, *Submission 47*; Telstra, *Submission 45*; Australian Bankers' Association, *Submission 27*.

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

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

61 See Ch 7.

statutory action into the existing legislative and common law framework of tort law. This approach is preferable to the establishment of an entirely separate legislative framework,[62] or to leaving these issues open and therefore uncertain in key respects.

Abolition of common law actions

4.55 The Terms of Reference ask whether, in the event that the statutory action were enacted, any common law actions should be abolished. Such a provision may be unnecessary, depending on common law developments at the time of enactment.

4.56 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.

4.57 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.[63]

4.58 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.

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

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

5. Two Types of Invasion

Contents

Summary 73
A cause of action for two types of invasion of privacy 74
Intrusion upon seclusion 76
    Intrusion in the United States 77
    Intrusion in the United Kingdom 78
    Intrusions in New Zealand 80
Misuse of private information 81
    Misuse in other jurisdictions 81
    Misuse or disclosure? 82
    Untrue personal information 83
Examples 85
False light and appropriation 87
An open-ended action? 88
One cause of action, not two 89

Summary

5.1 The ALRC recommends that for an action under the new tort, a plaintiff must prove that their privacy was invaded in one of the following ways:

(a) intrusion upon seclusion; or

(b) misuse of private information.

5.2 Intrusion upon seclusion will usually involve watching, listening to, or recording someone's private activities or private affairs. It can also involve unwanted physical intrusion into someone's private space. Examples might include taking a photo of someone in a change room, reading their bank statements, tapping their phone calls, or hacking into their computer.

5.3 Misuse of private information will usually involve collecting or disclosing someone's private information. Examples might include publishing a person's medical records in a newspaper or posting sexually explicit photographs of someone on the internet, without their permission.

5.4 These two categories 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 cause of action.

5.5 The two types of invasion may sometimes overlap: taking a photo of a person in the bathroom may be both an intrusion into their seclusion, as well as a wrongful collection of private information. Perhaps more often, a misuse of private information will follow an intrusion upon seclusion: a photo will be wrongly published, after it was wrongly taken.

5.6 Confining the tort to these two types of invasion of privacy will make the scope of the tort more certain and predictable. Invasions of privacy that do not fall into one of these two categories of invasion will not be actionable under this statutory tort.

5.7 This first element of the tort cannot be considered in isolation, because much turns on the question of what is 'private'. To determine what is private in a particular case, the second element of the tort must be considered, namely, whether a person in the position of the plaintiff would have a reasonable expectation of privacy. This is discussed in Chapter 6.

5.8 In other chapters of this Report, the ALRC recommends that the invasion of privacy must be committed intentionally or recklessly, must be found to be serious, and must not be justified by broader public interest considerations, such as freedom of speech.

A cause of action for two types of invasion of privacy

Recommendation 5–1 The Act should provide that the plaintiff must prove that his or her privacy was invaded in one of the following ways:

(a) intrusion upon seclusion, such as by physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs; or

(b) misuse of private information, such as by collecting or disclosing private information about the plaintiff.

5.9 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 outside Australia relating to invasions of privacy, relate either to an intrusion upon seclusion or a misuse of private information.

5.10 To provide clarity, certainty and guidance about the purpose and scope of the new action, the ALRC recommends that the action be explicitly confined to these two

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]. See also 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.

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] This should help address the common concern among some stakeholders that a new tort might be uncertain.[4]

5.11 The two categories of invasion of privacy recommended above draw on the well-known categorisation of privacy torts in the United States (US), first set out by William Prosser in 1960, and followed in the US *Restatement of the Law (Second) of 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 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]

5.12 Prosser's taxonomy focused on tort law, but there are other more general privacy taxonomies. US scholar Daniel Solove looked more broadly at 'the different kinds of activities that impinge upon privacy' and discovered 'four basic groups of harmful activities', each of which 'consists of different related subgroups of harmful activities':

(1) **Information collection:** surveillance, interrogation;

(2) **Information processing:** aggregation, identification, insecurity, secondary use, exclusion;

(3) **Information dissemination:** breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion;

(4) **Invasion:** intrusion, decisional interference.[7]

5.13 Solove's taxonomy highlights that many harmful activities may be characterised as invasions of privacy. A general legal action for invasion of privacy would therefore seem to be too broad and imprecise.[8] Gleeson CJ said in *ABC v Lenah Game Meats*

---

2 This is similar to the approach recommended by the Victorian Law Reform Commission (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 That privacy laws should be clear and certain is one of the ALRC's guiding principles: see Ch 3.

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

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

7 Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477.

8 This is discussed later in this chapter.

that 'the lack of precision of the concept of privacy is a reason for caution in declaring a new tort of the kind for which the respondent contends'.[9]

5.14 Dr Nicole Moreham has identified two 'overarching categories' covering six different ways of breaching privacy.[10] The first overarching category is unwanted watching, listening, recording and disseminating of recordings—namely, intrusion. The second is obtaining, keeping and disseminating private information—which 'have at their heart the misuse of private information'.[11]

5.15 The ALRC recommends that, in Australia, a new privacy tort should be confined to two broad categories of invasion of privacy, similar to the first two of Prosser's four categories and similar to Moreham's two overarching categories: (1) intrusion upon seclusion; and (2) misuse of private information. 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"'.[12] These two types of invasion of privacy are discussed further below.

5.16 It should be noted that this element of the tort cannot be satisfied without considering the second element of the tort, recommended in Chapter 6: whether a person in the position of the plaintiff would have a reasonable expectation of privacy, in all of the circumstances. The two elements will need to be considered together. In determining whether this element is satisfied, courts will usually consider whether there has been an intrusion into the *private* space, *private* activities or *private* affairs of the plaintiff, or a misuse of *private* information. The question of what is private in a particular case should be determined by asking whether a person in the position of the plaintiff would have had a reasonable expectation of privacy.

Intrusion upon seclusion

5.17 Intrusion upon seclusion is one of the two most commonly recognised categories of invasion of privacy. It is essential that the new tort for serious invasions of privacy capture this type of conduct.

5.18 Intrusions upon seclusion usually refer to intrusions into a person's *physical* private space. Watching, listening to and recording another person's private activities are the clearest and most common examples of intrusion upon seclusion. They are the types of activities the ALRC intends should be captured by this limb of the tort. To make this clear, the ALRC recommends that these types of intrusion be specifically included in the Act, as examples of intrusion upon seclusion. The examples are intended to clarify, but not limit, the meaning of 'intrusion upon seclusion'.

---

9 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [41].

10 Nicole Moreham, 'Beyond Information: The Protection of Physical Privacy in English Law' (2014) 73(2) *Cambridge Law Journal* (forthcoming).

11 Ibid.

12 *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.

5.19 Intrusion upon seclusion aligns with Moreham's second overarching category of invasion of privacy. Moreham writes:

> Peering through a person's bedroom window, following her around, bugging her home or telephone calls, or surreptitiously taking for one's own purposes an intimate photograph or video recording are all examples of this kind of intrusion.[13]

5.20 Although watching and listening to private activity may be an invasion of privacy, it might often not be serious. Recording a private activity is clearly less justifiable, and more likely to be a serious invasion of privacy. This is partly because the recording may later be distributed, although this may be considered a separate wrong. If the recording is not distributed, or shown to anyone else, it may nevertheless be watched or listened to later by the person who made the recording.

5.21 It is important not to look at these elements in isolation. To have an action, the plaintiff must also have a reasonable expectation of privacy, the intrusion must have been both intentional or reckless and serious, and the intrusion must not be in the public interest.

5.22 In many cases there is no legal redress in Australia for intrusions upon seclusion, because of the limitations of other tort actions.[14] The tort of intrusion upon seclusion, Prosser wrote in 1960 concerning US law, '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'.[15] These gaps in privacy protection remain in Australia today. The Office of the Victorian Privacy Commissioner submitted that a large number of individuals contact its office seeking redress for interferences with spatial or physical privacy, 'for which there is currently no readily accessible remedy in Australian law':

> Increasingly, people are becoming concerned about intrusions into their spatial privacy, particularly given the rise in surveillance technologies. The Privacy Commission receives hundreds of complaints each year relating to spatial privacy. In many cases (eg, in situations where surveillance is conducted by an individual or small business, or where information is not recorded) such intrusions will not be covered by current information privacy laws.[16]

Intrusion in the United States

5.23 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'.[17] 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

13 Moreham, above n 11, 1.
14 See Ch 3.
15 Prosser, above n 7, 392.
16 Office of the Victorian Privacy Commissioner, *Submission 108*.
17 Prosser, above n 7, 389–92; *Jones v Tsige* (2012) ONCA 32.

employment' and another case of 'unauthorized prying into the plaintiff's bank account'.[18]

5.24 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.

5.25 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.[19]

5.26 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.'[20]

Intrusion in the United Kingdom

5.27 The tort of invasion of privacy by intrusion upon seclusion is less clearly recognised in the United Kingdom (UK), but this appears to be changing.[21] Professor Chris Hunt has noted a recent trend in cases suggesting 'English law is evolving to capture intrusions'.[22] After journalists intruded into the hospital room of the actor Gordon Kaye and took photos of the injured man, the English Court of Appeal in 1990 held that he had no right to privacy as such in English law. And in 2004, the House of Lords in *Wainwright v Home Office*[23] 'expressly declined to recognize a general right

---

18 Prosser, above n 7, 389–92.
19 American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652B.
20 Warby et al, above n 2, [3.68].
21 '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.
22 Chris Hunt, 'Refining Privacy in Tort Law by Patrick O'Callahan' (2014) 73 *Cambridge Law Journal* 178.
23 *Wainwright v Home Office* [2004] 2 AC 406.

to privacy which would extend to physical privacy interferences not involving the dissemination of information'.[24] But in a book review published in 2014, Hunt writes that it 'seems inevitable that English courts would in fact provide a remedy to a claimant in Kaye's situation if the case were decided today'.[25]

5.28 Discussing the 'curious' resistance of the English courts to recognise a cause of action for intrusion, Professor 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 [of the *European Convention on Human Rights*], 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![26]

5.29 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 Hoffmann 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'.[27] 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'.[28]

5.30 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,[29] but also in the effect the publication will have on the claimant's and related parties' lives after publication.[30] Intrusive behaviour by the UK media led to the Leveson Inquiry into the Culture, Practice and Ethics of the Press.[31]

5.31 It remains to be seen whether a separate cause of action for intrusion upon seclusion will be recognised at common law in the UK.[32] The authors of *Gurry on Breach of Confidence* note that the case for recognising a separate *tort* of privacy, as

---

24 Warby et al, above n 2, [10.04].
25 Hunt, above n 23.
26 Wacks, above n 22, 247 (citations omitted).
27 *Campbell v MGN Ltd* [2004] 2 AC 457, [75].
28 *Murray v Big Pictures (UK) Ltd* [2009] Ch 481, [36]. See, also, Warby et al, above n 2, [10.06].
29 See, further, Moreham, above n 11; *Tsinguiz v Imerman* [2010] EWCA Civ 908 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.
30 *Goodwin v NGN Ltd* [2011] EWHC 1437 (QB); *Mosley v United Kingdom* [2011] ECHR 774; *A v United Kingdom* [2002] ECHR 811; [2003] EHRR 51.
31 See, further, *The Leveson Inquiry* <www.levesoninquiry.org.uk>.
32 See, further, Moreham, above n 11.

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.[33]

5.32 In any event, any gap in the UK law may not be as 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.[34]

Intrusions in New Zealand

5.33 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 to record 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 prospect of publicity, is an actionable tort in New Zealand'.[35] The court concluded that it was. An intrusion tort was a 'logical extension or adjunct' to the tort for misuse of private information.[36] Whata J said that the court 'can apply, develop and modify the tort to meet the exigencies of the time'.[37]

5.34 In defining the ingredients of the tort, Whata J drew guidance from the decision of the Ontario Court of Appeal in *Jones v Tsige*,[38] 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.[39]

5.35 This closely resembles the tort recommended in this Report. Including intrusion upon seclusion as one of the two types of actionable invasion of privacy in the new tort would remedy one of the key deficiencies in Australian law identified in Chapter 3.

---

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

34 In Ch 15, the ALRC recommends the introduction of a statutory tort of harassment, in the event that the privacy tort is not introduced.

35 *C v Holland* 3 NZLR 672, [1].

36 Ibid [86].

37 Ibid.

38 *Jones v Tsige* (2012) ONCA 32. In this case, 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.

39 *C v Holland* 3 NZLR 672, [94]–[95] (Whata J).

Misuse of private information

5.36 The second type of invasion of privacy that the ALRC recommends should be covered by the new privacy tort is misuse of private information. This should be neither surprising nor contentious. Misuse of private information is a widely recognised type of invasion of privacy, already actionable in the UK, the US, New Zealand, Canada and elsewhere. No stakeholder suggested that if a new privacy tort were enacted in Australia, it should not cover misuse of private information.

5.37 Most cases involving private information are concerned with unauthorised disclosure. 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.[40] But there are other ways of misusing private information, including wrongfully obtaining it. The ALRC recommends that the Act include the two most common types of misuse of private information as illustrative examples: collecting or disclosing private information.

5.38 This corresponds to the second of Moreham's two overarching categories of invasion of privacy, under which Moreham found three sub-categories of invasion. It was a breach of privacy to:

> (1) *'find out* things about others that they wish to keep to themselves, by acquiring bank records, reading diaries, or hacking e-mails, for instance';
>
> (2) '*keep* that private information either for one's own future reference or to share it with others'; and
>
> (3) *disclose* private information to another, for example 'by uploading it onto the internet, disseminating it in the media or passing it on through gossip'.[41]

5.39 'The objection in these cases,' Moreham writes, 'is to the fact that someone is finding out about you against your wishes. She is reading your private records, building up a file or dossier about you or, by disseminating private information, allowing others to do the same'.[42]

Misuse in other jurisdictions

5.40 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'.[43] The commentary to the *Restatement* notes that publicity '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'.[44]

---

40 *Campbell v MGN Ltd* [2004] 2 AC 457, [51].
41 Moreham, above n 11, 3.
42 Ibid.
43 American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652D.
44 Ibid (commentary on § 652D).

5.41 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).[45] 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 art 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.

5.42 The New Zealand courts have recognised a new tort of invasion of privacy by giving publicity to private facts.[46] There are two fundamental requirements for a successful claim. The first is the 'existence of facts in respect of which there is a reasonable expectation of privacy'.[47] The second is 'publicity given to those private facts that would be considered highly offensive to an objective reasonable person'.[48]

Misuse or disclosure?

5.43 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'.[49]

5.44 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'.[50]

5.45 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 (or fellow employee)[51] may have intruded into the private affairs of that customer. Such an intrusion would be covered by the first category of invasion recommended 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.

---

45 *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).
46 *Hosking v Runting* (2005) 1 NZLR 1.
47 Ibid [117] (Gault P and Blanchard J).
48 Ibid.
49 Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1108.
50 Wacks, above n 22, 247, quoting Lord Hoffmann in *Campbell*.
51 See, eg, *Jones v Tsige* (2012) ONCA 32.

5.46 Public disclosure of private information will be a common type of misuse, but the Act should not confine misuse to public disclosures. In some circumstances, the disclosure of personal information to one other person may be a serious invasion of privacy.[52]

5.47 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'.[53]

5.48 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 cases in which it is reasonable to expect one's personal information not to be disclosed even within a small circle.[54]

Untrue personal information

Recommendation 5–2 The Act should provide that 'private information' includes untrue information, but only if the information would be private if it were true.

5.49 A person's privacy can in some cases be invaded by the disclosure of untrue information, but perhaps this would only amount to an invasion of privacy if the information were true. For example, a court might consider that the fact that a particular person, an ordinary citizen, is suffering from a mental illness is private information which should not be disclosed in the press. If a newspaper disclosed that a particular person had a mental illness, and it turned out that the person did not, then an action for invasion of privacy should not be defeated merely on the basis that the information was incorrect.

5.50 This is one reason why the ALRC recommends 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.

52 Further, disclosure is not the only type of misuse of private information.
53 American Law Institute, *Restatement of the Law Second, Torts* (1977).
54 See, eg, *Giller v Procopets* (2008) 24 VR 1.

5.51 This position is consistent with the *Privacy Act 1988* (Cth), in which personal information is defined in s 6 to include information or an opinion 'whether true or not'.[55] It is also the position in UK law. Former judge of the UK High Court, Sir 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.[56]

5.52 In *McKennitt v Ash*, Longmore LJ of the English Court of Appeal stated:

> 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 is an irrelevant inquiry in deciding whether the information is entitled to be protected and judges should be chary of becoming side-tracked into that irrelevant inquiry.[57]

5.53 Dr Normann Witzleb submitted that 'the misuse or disclosure of untrue private information can be just as damaging as the misuse or disclosure of true private information':

> There is no reason to limit the protection to true information. Limiting the tort to true information would require a plaintiff to confirm or admit in court the veracity of information which she would not like to see in the public domain, at all. This would be likely to unfairly prejudice the plaintiff's interests in protecting her private life from publicity.[58]

5.54 Sometimes the disclosure of untrue private information will amount to defamation, but often it may not. The ALRC does not consider, as one stakeholder suggested, that the law of defamation provides 'adequate protection to individuals for information that is found to be incorrect'.[59]

5.55 Also, it should be stressed that for the plaintiff to have an action under the privacy tort in this Report, the other elements of the tort would of course have to be satisfied. The untrue information would have to be a matter about which the plaintiff had a reasonable expectation of privacy and the misuse would have to be serious.[60] The ALRC is not recommending a tort for the publication of untrue information or, as discussed below, a tort for placing a person in a 'false light'.

---

55 *Privacy Act 1988* (Cth).

56 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'.

57 *McKennitt v Ash* [2008] QB 73, [86]. This was quoted in N Witzleb, *Submission 116*.

58 N Witzleb, *Submission 116*.

59 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

60 See Chs 6 and 8.

Examples

5.56 Examples of invasion of privacy should provide additional guidance and certainty. The ALRC recommends that brief and general examples of certain types of invasion of privacy be included in the Act.

5.57 For intrusion upon seclusion, the ALRC recommends the Act include the following: 'such as by physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs'.

5.58 For misuse of private information, the ALRC recommends the Act include the following: 'such as by collecting or disclosing private information about the plaintiff'.

5.59 A number of stakeholders in the current Inquiry said a non-exhaustive list of examples should be included in the new provision,[61] stressing that this would provide courts, parties and business with some guidance and certainty.[62] Some stakeholders said that the examples should be general and flexible, so that the action could 'evolve with social and technological developments'.[63]

5.60 Candice Jansz-Richardson said the examples should be 'relatively general in nature to ensure their ability to translate over time'.[64] The Public Interest Advocacy Centre (PIAC) submitted that examples should be 'open-ended and inclusive, which would build sufficient flexibility into the recommended cause of action for it to be appropriately adapted to changing social and technological circumstances'.[65] 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'.[66]

5.61 Other stakeholders said that the cause of action should not include a list of examples.[67] 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

---

61 N Witzleb, *Submission 116*; N Henry and A Powell, *Submission 104*; 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*.

62 Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 97*; 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*.

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

64 C Jansz-Richardson, *Submission 24*.

65 Public Interest Advocacy Centre, *Submission 105*; Public Interest Advocacy Centre, *Submission 30*.

66 Australian Privacy Foundation, *Submission 39*.

67 ASTRA, *Submission 99*; P Wragg, *Submission 73*; SBS, *Submission 59*; ASTRA, *Submission 47*; ABC, *Submission 46*; Law Institute of Victoria, *Submission 22*; Pirate Party of Australia, *Submission 18*; P Wragg, *Submission 4*.

actionable.[68] It was also suggested that the examples in the list might become outdated.[69] Other stakeholders suggested that examples were unhelpful because privacy was 'contextual and depends on facts and circumstances'.[70] 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'.[71] SBS submitted that 'the key for any statutory cause of action is flexibility', warning that:

> 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.[72]

5.62 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'.[73] Drs Nicola Henry and Anastasia Powell said examples in the Act should include 'technology-facilitated sexual violence and harassment'.[74]

5.63 One Victorian legal service recommends the following examples:

> a person's online accounts such as their email account or social media account has been accessed, interfered with or misused; a person's private information, including photographs or personal details, have been accessed or disclosed; an individual's private email correspondence or telephone calls have been monitored or recorded; or an individual's movements and locations have been monitored and tracked, for example via mobile technology.[75]

5.64 In its 2008 privacy report, the ALRC also recommended that examples be included in a statute providing for a cause of action for serious invasion of privacy; where

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

---

68 Law Institute of Victoria, *Submission 22*; P Wragg, *Submission 4*. The Law Institute of Victoria submitted that the inclusion of a list 'might give would-be defendants the impression that conduct outside the parameters of the list does not constitute an invasion of privacy'.

69 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'.

70 Ibid.

71 ABC, *Submission 46*.

72 SBS, *Submission 59*.

73 Electronic Frontiers Australia, *Submission 44*.

74 N Henry and A Powell, *Submission 104*.

75 Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 97*.

- sensitive facts relating to an individual's private life have been disclosed.[76]

5.65 The ALRC considers many of the examples provided by stakeholders and in its past report to be good examples of serious invasions of privacy. Some would clearly be covered by the examples recommended above.

5.66 Some examples suggested above are more specific and descriptive. The ALRC considers that the application of the tort to particular circumstances is best left to the courts to consider on a case by case basis. Specific examples may provide additional guidance, but may risk distracting the court from the consideration of the distinct facts and circumstances of a particular case.

False light and appropriation

5.67 The cause of action in this Report is not designed to capture the two other so-called 'privacy torts' in the United States, namely, 'publicity which places the plaintiff in a false light in the public eye' and 'appropriation, for the defendant's advantage, of the plaintiff's name or likeness'.[77]

5.68 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.[78]

5.69 The disclosure of private facts and unreasonable intrusion upon seclusion concern the key privacy interests, such as personal dignity and autonomy, whereas the other US torts arguably protect other 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.[79]

---

76 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–1.

77 Prosser, above n 7, 392.

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

79 Ibid, 256 (Gummow and Hayne JJ).

5.70 The tort of passing off does not provide full protection of people's image rights,[80] but the ALRC considers that reform to the law relating to image rights would need to be considered more broadly and in the context of Australia's intellectual property law.

5.71 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'.[81] Prosser himself wrote that the 'false light cases obviously differ from those of intrusion, or disclosure of private facts':

> The interest protected is clearly that of reputation, with the same overtones of mental distress as in defamation.[82]

5.72 In the US, Prosser's formulation of appropriation as a privacy tort is contentious and often described as a 'right of publicity'. The Supreme Court of Colorado has noted that Prosser's formulation of the tort

> subsumed the two types of injuries—personal and commercial—into one cause of action that existed under the misleading label of 'privacy'. The privacy label is misleading both because the interest protected (name and/or likeness) is not 'private' in the same way as the interests protected by other areas of privacy law and because the appropriation tort often applies to protect well-known 'public' persons.[83]

5.73 It should be noted that putting someone in a false light or appropriating their name or likeness may, in some cases, also be a serious invasion of a person's privacy under the tort designed in this Report. For example, the Domestic Violence Legal Service and the North Australian Aboriginal Justice Agency noted the 'common scenario in domestic violence cases where the perpetrator hacks into the victim's existing social media account or creates a false social media account in the name and or image of the victim and then posts material purporting to be authored by the victim'.[84] The ALRC considers that, depending on the circumstances, this may be both an intrusion into seclusion (hacking into a person's social media account) and a misuse of private information (posting private photos). The tort in this Report is certainly not designed to deny relief where the plaintiff has been put in a false light, or had their name or likeness appropriated. But it is not intended to capture these other wrongs per se. Other causes of action will more directly relate to these wrongs.

An open-ended action?

5.74 Some stakeholders submitted that the new tort should be framed more broadly—that it should not be confined to intrusions upon seclusion and misuse of private information. They favoured a single cause of action, often because this was thought to

---

80 To have an action under the tort of passing off, the plaintiff or the plaintiff's business must have 'a certain goodwill or reputation' and must suffer 'injury in his trade or business': *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd* (1981) 1 NSWLR 196, [204].

81 Wacks, above n 22, 181.

82 Prosser, above n 7, 400.

83 *Joe Dickerson & Associates, LLC v Dittmar 34 P3d 995 (Supreme Court of Colorado, 2001, Bender J)*.

84 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*.

make the action more flexible—that is, open to invasions other than by misuse of personal information or intrusion upon seclusion.[85] Witzleb, for example, said the action should be formulated broadly, to leave its further development to the courts.[86] The Australian Privacy Foundation likewise said that introducing two torts may result in some privacy breaches not being covered.[87] The Office of the Australian Information Commissioner (OAIC) supported the enactment of 'a single and comprehensive tort', rather than one confined to intrusion upon seclusion and misuse of private information. The OAIC said that confining the tort 'risks leaving gaps in privacy protection' and makes the tort less flexible and adaptive to new technologies and practices'.[88]

5.75 Other stakeholders stressed the need for certainty. For example, Telstra submitted that the 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'.[89]

5.76 The ALRC considers that the 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 and targeted. The ALRC recommends 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. Arguing for even greater prescription and certainty than the ALRC recommends, Professor Kit Barker submitted that

> generalised causes of action give great discretion and little guidance to judges. More discrete, lower-level rules provide higher levels of guidance and greater predictability. Joseph Raz is notorious for preferring rules to general principles for precisely these reasons. They give greater respect to the rule of law.[90]

5.77 As discussed below, greater guidance could, in theory, also be achieved by enacting two separate and tailored causes of action, but the ALRC considers this to be unnecessary.

One cause of action, not two

5.78 The ALRC recommends 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 actions would be substantially different—that is, have different elements, defences and remedies. The ALRC considers that separate actions are not necessary.

---

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

86 N Witzleb, *Submission 29*.

87 Australian Privacy Foundation, *Submission 39*.

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

89 Telstra, *Submission 45*. However, Telstra opposes even a more confined privacy tort.

90 K Barker, *Submission 126*.

5.79 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.[91]

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

5.81 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'.[92]

5.82 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.

5.83 Some stakeholders argued that there are important differences between intrusions upon seclusion and misuse of private information, and that these differences suggest there should be two separate and tailored causes of action. Barker submitted that there should be separate causes of action because they should have different fault elements.[93] However, as discussed in Chapter 7, the ALRC considers that they should have the same fault element—they should only be actionable where the conduct of the plaintiff was intentional or reckless.

5.84 Importantly, as Hunt has argued, having a single action also 'avoids the problem of discordant principles emerging between the two actions, which would be undesirable since they protect the same interest'.[94]

5.85 The ALRC considers the cause of action designed in this Report to be flexible enough to deal with both types of invasion of privacy, while providing sufficient guidance and certainty.

---

91 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.126].

92 I Turnbull, *Submission 5*.

93 K Barker, *Submission 126*.

94 Chris DL Hunt, 'Privacy in the Common Law: A Critical Appraisal of the Ontario Court of Appeal's Decision in *Jones v Tsige*' (2012) 37 *Queen's LJ* 665, 673.

6. Reasonable Expectation of Privacy

Contents

Summary 91
A test for what is private 92
Highly offensive? 95
Relationship with other elements and defences 95
Considerations 96
Different for misuse and intrusions 97
Nature of the information 98
Means used 100
Place of intrusion 100
Purpose of intrusion 102
How information was held or communicated 102
Information in the public domain 103
Attributes of the plaintiff 104
Conduct of the plaintiff 105
Other matters 107

Summary

6.1 The ALRC recommends 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 essentially an objective test used to answer the question 'Is this private?' The subjective expectation of the plaintiff may be a relevant consideration, but it is not the focus of the inquiry. The question is determined by the court, after close analysis of the particular circumstances of the case.

6.3 The ALRC also recommends that the Act include a non-exhaustive list of factors that a court may consider when determining whether a person would have had a reasonable expectation of privacy. This is intended to provide guidance and assistance to the parties and the court, without limiting the matters that might be considered in a particular case.

6.4 The recommended factors include: the nature of the private information; the means used to obtain the private information or to intrude upon seclusion; the place where the intrusion occurred; the purpose of the misuse or intrusion; how the private information was held or communicated; whether the private information was already in the public domain; the attributes of the plaintiff, such as their age; and the conduct of the plaintiff.

A test for what is private

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

6.5 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 recommends 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.

6.6 This is preferable to attempting to define 'privacy' in the Act as it is notoriously difficult to define. 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]

6.7 The test recommended by the ALRC is an objective one. The court must consider, not whether the plaintiff subjectively expected privacy, but whether it would be reasonable for a person in the position of the plaintiff to expect privacy. The subjective expectation of the plaintiff may be a relevant consideration, particularly if that expectation was made manifest, but it is not the focus of the test, nor an essential element that must be satisfied.[2]

6.8 In determining whether a person would have a reasonable expectation of privacy, the court should consider 'all of the circumstances'. Some of these circumstances will relate to the position of the particular plaintiff, and therefore to this extent the test has a subjective element. More broadly, the phrase 'all of the circumstances' highlights that whether this test will be satisfied will depend very much on the facts of each particular case.

---

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

2 Expectation of privacy has for this reason been called a normative rather than a descriptive standard. 'Suggestions that a diminished subjective expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed. It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a subjective expectation of privacy and thereby forfeits the protection of s 8 [*Human Rights Act 1998* (UK)]. Expectation of privacy is a normative rather than a descriptive standard': *R v Tessling* [2004] 3 SCR 432 (Binnie J).

6.9 The 'reasonable expectation' test was supported by a number of stakeholders.[3] It was said to be flexible and able to adapt to new circumstances.[4] This is important, because community expectations of privacy 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'.[5] The Australian Interactive Media Industry Association submitted that the reasonable expectation requirement was 'an important mechanism by which to ensure that only sensible and genuine privacy matters are able to access the courts and seek redress'.[6]

6.10 Similar tests have been recommended in reports of the ALRC, the NSW Law Reform Commission (NSWLRC) and the Victorian Law Reform Commission (VLRC).[7] This test is also used in a number of other jurisdictions. It has been adopted in the United Kingdom (UK), New Zealand, and several Canadian provinces.[8]

6.11 In *Campbell v MGN*, 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'.[9] Lord Hope said that the 'question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity'.[10]

6.12 Some stakeholders opposed the use of a reasonable expectation test,[11] with some saying that the test was too vague.[12] In the ALRC's view, the test must be flexible, but not uncertain. Courts are used to determining issues of reasonableness or even reasonable expectation in other contexts.[13]

---

3 Australian Interactive Media Industry Association (AIMIA), *Submission 125*; Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; T Butler, *Submission 114*; Google, *Submission 91*; J Chard, *Submission 88*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; 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*; ASTRA, *Submission 47*; Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Optus, *Submission 41*; Australian Privacy Foundation, *Submission 39*; 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*; Women's Legal Centre (ACT & Region) Inc, *Submission 19*; Insurance Council of Australia, *Submission 15*.

4 Office of the Victorian Privacy Commissioner, *Submission 108*; ASTRA, *Submission 99*.

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

6 Australian Interactive Media Industry Association (AIMIA), *Submission 125*.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–2; Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Recs 25, 26; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 20–26.

8 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, 2011) 17–21.

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

10 Ibid [99].

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

12 Australian Bankers' Association, *Submission 27*.

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

6.13 Professor Eric Barendt has said the test is artificial.[14] He wrote that in 'many cases a claimant will have had no actual expectations at the time his privacy was infringed'.[15] The ALRC considers that, although the subjective expectations of the plaintiff may sometimes be relevant, the focus of the test should be on whether a reasonable person would expect privacy, not whether the plaintiff in fact expected privacy. To make this clearer, the ALRC recommends that the Act refer to whether a 'person in the position of the plaintiff' would have a reasonable expectation of privacy.

6.14 The ALRC also considers that there are notable benefits in 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 United States (US).

6.15 Some stakeholders, while supporting a reasonable expectation of privacy test, nevertheless expressed some concern that expectations of privacy may be considered to have fallen, perhaps following common and unchallenged industry practices. The concern was that, because technologies and services would increasingly encroach into people's private lives, people will then either actually expect less privacy, or it will increasingly seem unreasonable to expect the same level of privacy. There is a concern that privacy standards would erode.[16]

6.16 However, as noted above, other stakeholders considered that its ability to adapt to community standards to be one of the strengths of the reasonable expectation of privacy test. For example, the Australian Subscription Television and Radio Association (ASTRA) noted the 'evolution of society's understanding of what is a private matter since the advent of publicly available social media profiles'.[17]

6.17 Community expectations of privacy no doubt change, but the ALRC considers that a privacy tort must be able to adapt to such changes. Legislative privacy standards cannot be set in stone. But this does not mean the standards are infinitely flexible, or that it might soon be unreasonable to expect any privacy. Privacy has been valued by so many for so long that not only is it not dead, as some have dramatically claimed, but it should continue to be reasonable to expect privacy in many circumstances.

6.18 Although there is a separate element of the tort that explicitly confines the tort to 'serious' invasions of privacy,[18] the 'reasonable expectation of privacy' test should also help ensure that non-serious privacy interests are not actionable under the tort.

---

14 Eric Barendt, 'A Reasonable Expectation of Privacy?' A Coherent or Redundant Concept?' in Andrew Kenyon (ed) (forthcoming, 2014).

15 Ibid. Barendt raises other concerns. For example, he writes that courts might be tempted to consider matters when applying this test, when those matters should instead be considered when balancing privacy with freedom of expression: Ibid. The ALRC acknowledges the potential for overlap between this test and other elements and defences in the new tort.

16 See, eg, Australian Privacy Foundation, *Submission 110*.

17 ASTRA, *Submission 99*.

18 See Ch 8.

Highly offensive?

6.19 In *ABC v Lenah Game Meats*, Gleeson CJ proposed a different test for what is private:

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. 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.[19]

6.20 This passage was referred to, a number of times, in opinions of the House of Lords in *Campbell*. Lord Nicholls 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 which publication was a matter of proper public concern. This could be a recipe for confusion.[20]

6.21 Baroness Hale also preferred an objective reasonable expectation test, saying that it was 'much simpler and clearer' than an offensiveness test of privacy.[21] 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.[22]

6.22 The ALRC considers that the offensiveness of a disclosure or intrusion should be one matter able to be considered by a court in determining whether there is a reasonable expectation of privacy. It is more reasonable to expect privacy, where a breach of privacy would be considered highly offensive. As discussed in Chapter 8, offence may also be used to distinguish serious invasions of privacy from non-serious invasions of privacy.

Relationship with other elements and defences

6.23 Some matters will be relevant to the reasonable expectation of privacy test and also to other elements and defences of the tort.

---

19 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42].
20 *Campbell v MGN Ltd* [2004] 2 AC 457, [22].
21 Ibid [135].
22 Ibid [136].

6.24 For example, some public interest matters may be considered when determining whether the plaintiff had a reasonable expectation of privacy, even though the ALRC recommends that the tort feature a separate public interest test. In some cases, a public interest matter will be so conspicuous that it may not be sensible to ignore it when determining whether the plaintiff has a reasonable expectation of privacy.

6.25 Other matters may be the subject of a separate defence. For example, a separate defence for consent is recommended in Chapter 11. However, evidence of consent to the relevant conduct or related or similar conduct may also affect whether the plaintiff had a reasonable expectation of privacy.

Considerations

Recommendation 6–2 The 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, such as in the plaintiff's home;

(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, occupation and cultural background; and

(h) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy.

6.26 The ALRC recommends 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.

6.27 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.[23]

23 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill, cl 74(3)(a).

6.28 A number of stakeholders submitted that the Act should include a list of factors for a court to consider,[24] and many generally supported the factors recommended in the Discussion Paper.[25] Others suggested that the reasonable expectation of privacy test would remain uncertain even if such a list of factors were included.[26] However, the ALRC considers that the lack of a comprehensive definition of privacy should not be a reason for denying remedies to people whose privacy is clearly invaded in certain ways.

6.29 In *Murray v Big Pictures*, which concerned photographs taken of a child in the street for commercial publication, the High Court of England and Wales 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.[27]

6.30 Other matters will be relevant in other cases, particularly in cases concerning intrusion upon seclusion. Professor Raymond 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
>
> (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).[28]

Different for misuse and intrusions

6.31 Before discussing the different factors, it should be noted that the factors that will be relevant to the reasonable expectation of privacy test may differ, depending on whether an invasion of privacy was by misuse of private information, or by intrusion

---

24 See, eg, Public Interest Advocacy Centre, *Submission 105*; Insurance Council of Australia, *Submission 102*; Office of the Victorian Privacy Commissioner, *Submission 108*.

25 See, eg, Public Interest Advocacy Centre, *Submission 105*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Guardian News and Media Limited and Guardian Australia, *Submission 80*. AIMIA said the ALRC's factors 'recognise that privacy is contextual in nature': Australian Interactive Media Industry Association (AIMIA), *Submission 125*.

26 Eg, the Australian Bankers' Association submitted that a 'shopping list' of criteria would be 'of little use unless there is complete clarity about exactly what "privacy" is'... [T]his approach increases the risk of uncertainty for business and the community': Australian Bankers' Association, *Submission 84*.

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

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

upon seclusion. As Associate Professor Paul Wragg submitted, a court's approach to determining whether a person in the position of the plaintiff would have a reasonable expectation of privacy is likely to be 'markedly different in intrusion claims than informational claims'.[29] Within these broad categories of invasion, there are sub-categories, and the factors may also differ in relevance between those categories too.

6.32 In fact, which factors are relevant may differ in every case. As noted above, the test very much depends on the particular circumstances of the case. Different lists of factors could no doubt be created, for different types of invasion of privacy. But the ALRC considers that one list that is not exhaustive or prescriptive will be sufficient. Courts may consider the matters on the list that are relevant to the particular case, ignore those that are not, and consider any other matter that is relevant that is not on the list.

Nature of the information

6.33 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,[30] and financial matters are all likely to be private. Gleeson CJ said in *Australian Broadcasting Corporation v Lenah Game Meats* 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'.[31]

6.34 Personal information taken from medical records, reports, or interviews is also generally considered private in English courts.[32]

6.35 '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.[33]

6.36 The definition of 'sensitive information' in the *Privacy Act* may also be of some assistance to the courts, but should not be determinative of the question of whether the plaintiff had a reasonable expectation of privacy. '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

---

29 P Wragg, *Submission 73*.

30 Biometric data, such as a fingerprint, may also be private information. The OAIC submitted that the new tort should provide a remedy 'in the case of serious invasion of an individual's bodily privacy (such as in the case of unauthorised bodily testing'): Office of the Australian Information Commissioner, *Submission 90*.

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

32 M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [5.35].

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

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.[34]

6.37 This definition serves a particular regulatory purpose. It should be stressed that the types of sensitive information included in the definition will not *necessarily* give rise to a reasonable expectation of privacy under the tort. Whether something is private under the tort will depend on context and other relevant factors.

6.38 In the UK, it has been said that 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'.[35]

6.39 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'.[36]

6.40 However, intimate and family matters can extend beyond sexual matters. Professor Des 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'.[37] Butler also noted 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'.[38]

---

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

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

36 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.

37 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].

38 D Butler, *Submission 10*.

Means used

6.41 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 used spyware, or 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 suggest the plaintiff's privacy has been invaded (regardless of what personal information or photograph is taken).

6.42 ASTRA submitted that it is 'difficult to see how a person could form an expectation of privacy based on a use of technology of which they are unaware'.[39] However, the ALRC considers that a person can quite reasonably expect not to be intruded upon, even if they do not turn their minds to the means that might used to intrude upon their privacy. They may even reasonably expect privacy without even considering whether their privacy is remotely likely to be intruded upon at all.

6.43 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'.[40]

Place of intrusion

6.44 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. Most clearly, a person will have a greater expectation of privacy in the home than in a public place.

6.45 Although a person should generally have a lower expectation of privacy when in public, the ALRC considers that privacy may reasonably be expected in public places—in some circumstances.[41]

6.46 This has been recognised in a number of invasion of privacy cases outside Australia.[42] In one US case in 1964, a woman was photographed at a country fair leaving a 'fun house' at the moment at which some air jets blew her dress up. The photo was published on the front cover of a newspaper. The fact that she was in public, did not mean that she had no right to privacy. Harwood J of the Supreme Court of Alabama said:

> a purely mechanical application of legal principles should not be permitted to create an illogical conclusion. To hold that one who is involuntarily and instantaneously enmeshed in an embarrassing pose forfeits her right of privacy merely because she

---

39 ASTRA, *Submission 99*.

40 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.

41 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.

42 *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB); *Murray v Express Newspapers* [2008] EWCA Civ 446.

> happened at the moment to be part of a public scene would be illogical, wrong, and unjust.[43]

6.47 In an English case that went to the European Court of Human Rights, CCTV footage of a man in a public street, taken moments after he had tried to commit suicide, were later broadcast on television. The Court found this was an invasion of his privacy.[44] The man 'was in a public street but he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night, he was deeply perturbed and in a state of some distress'.[45] The footage was 'viewed to an extent which far exceeded any exposure to a passer-by or to security observation and to a degree surpassing that which the applicant could possibly have foreseen'.[46]

6.48 In *Campbell*, Naomi Campbell was also in a public place when she was photographed leaving a Narcotics Anonymous meeting. The publication of that photograph in a newspaper was found to be an invasion of her privacy.[47] Although Lord Hoffmann thought there was 'nothing embarrassing' about the particular picture, he did say that the

> the widespread publication of a photograph of someone which reveals him to be in a situation of humiliation or severe embarrassment, even if taken in a public place, may be an infringement of the privacy of his personal information.[48]

6.49 These cases illustrate some of the circumstances that may suggest that a person may have a reasonable expectation of privacy, despite being in a public place.

6.50 There may be different expectations of privacy with respect to the taking of a photo and to its later publication. It may be unreasonable to expect not to be photographed, particularly when in public,[49] but quite reasonable to expect the photograph not to be published, particularly if the photo captures a clearly private or humiliating moment. The importance of this distinction was stressed by photographers.[50]

6.51 Expectations of privacy may also vary between different types of public place. For example, a person may expect more privacy in a restaurant than when on the street.

6.52 Whether people can expect privacy at work is another interesting question. Although people should generally expect less privacy at work than at home, it is reasonable to expect some privacy at work. One case before the Supreme Court of California concerned whether a woman employed as a 'telepsychic' had invaded the privacy of one of her fellow employees—using, not her psychic powers, but a video camera hidden in her hat. The court found that the fact that other co-workers may have

---

43 *Daily Times Democrat v Graham,* 276 Ala 380 (1964) 478.
44 *Peck v United Kingdom* [2003] ECHR 44 (28 January 2003).
45 Ibid [62].
46 Ibid.
47 *Campbell v MGN Ltd* [2004] 2 AC 457.
48 Ibid [75].
49 Randerson J said the taking of photographs in a public place 'must be taken to be one of the ordinary incidents of living in a free community': *Hosking v Runting* (2005) 1 NZLR 1, [2003] NZHC 416, [138] (Randerson J).
50 Australian Institute of Professional Photography (AIPP), *Submission 95*.

witnessed the interactions and conversations did not mean the plaintiff could not have a reasonable expectation of privacy:

> In an office or other workplace to which the general public does not have unfettered access, employees may enjoy a limited, but legitimate, expectation that their conversations and other interactions will not be secretly videotaped by undercover television reporters, even though those conversations may not have been completely private from the participants' co-workers.[51]

Purpose of intrusion

6.53 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 their temperature, but may be invaded by a journalist entering the room to take photos of the patient for publication in a newspaper.[52]

6.54 In *Murray v Big Pictures*, the High Court of England and Wales 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'.[53] 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.[54]

6.55 *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'.[55]

6.56 The motivation of the defendant may also be relevant to an assessment of the seriousness of an invasion of privacy.[56]

How information was held or communicated

6.57 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.

---

51 *Sanders v American Broadcasting Companies Inc* (1999) 85 Calif. Rep. 2d 909. See, also, *Saad v Chubb Security Australia Pty Ltd* [2012] NSWSC 1183.

52 See, eg, *Kaye v Robertson* [1991] FSR 62.

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

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

55 Warby et al, above n 32, [5.123].

56 A malicious invasion of privacy, for example, may be more offensive and more serious. See Ch 8 for a discussion of the recommended 'seriousness' threshold.

6.58 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.[57]

6.59 New digital technologies will raise other questions. Email correspondence is treated like private correspondence, but not all information sent by email will be private in nature.

6.60 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 that the information is likely to be subject to a reasonable expectation of privacy.

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

Information in the public domain

6.62 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.

6.63 There may be no clear line between what is in the public domain and what is not. 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'.[58] 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.

6.64 Information that is private in nature 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

---

57 Warby et al, above n 32, [5.80].

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

> 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 people can still cause distress and damage to an individual's emotional or mental well-being.[59]

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

Attributes of the plaintiff

6.66 Some attributes of a plaintiff, such as age, may affect whether the person had 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'.[60]

6.67 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.

6.68 '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.[61] People who are reluctantly or involuntarily put in the public spotlight, such as the victim of a crime, may however be distinguished from those who seek the limelight.[62]

6.69 The NSWLRC also included in this list the 'extent to which the individual is or was in a position of vulnerability'.[63] 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 will also 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.[64]

6.70 The culture and background of a plaintiff may also be relevant to whether they have 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. For example, the cultural expectations of Aboriginal and Torres Strait Islander peoples and other cultural or ethnic groups may be relevant to the reasonable expectation of privacy in some circumstances. The Arts Law Centre of Australia

---

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

60 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].

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

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

63 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill cl 74(3)(a)(v).

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

stressed the importance of considering the 'confidential or culturally sensitive nature of cultural knowledge, stories, images of indigenous Australians'.[65]

6.71 The Australian Privacy Foundation said 'great care' should be given in taking into account age, occupation and other like factors, because it may suggest some people warrant less protection from invasions of privacy than others.[66] The ALRC agrees that the various factors should be considered carefully, when determining whether the plaintiff had a reasonable expectation of privacy, but it seems clear that some attributes of a plaintiff should give rise to a greater, or lesser, expectation of privacy.

Conduct of the plaintiff

6.72 The conduct of the plaintiff may sometimes affect whether the plaintiff had a reasonable expectation of privacy.

6.73 Some conduct may undermine a person's expectation of privacy. For example, if a plaintiff invited publicity about a particular matter, it may be less reasonable for them to expect the matter to be kept private. A person who runs naked on a football field can hardly expect not to be photographed.

6.74 A plaintiff cannot generally expect privacy where they have freely consented to the conduct that compromises their privacy.[67] In Chapter 11, the ALRC recommends that consent be a defence to this tort, but the plaintiff's consent to certain conduct may also arise when determining whether the plaintiff had a reasonable expectation of privacy. Consent given to someone other than the defendant can also be relevant. A plaintiff who has consented to the publication of private information in one newspaper, may not always reasonably expect the information not to be published in another newspaper.

6.75 A court might also ask whether the plaintiff had 'courted publicity on the relevant occasion'.[68] A person who has courted publicity cannot expect the same level of privacy as those who have not. However, care must be taken here, because it does not follow that such persons forgo any right to privacy, just as a person does not, by manifesting a desire for privacy, automatically become entitled to it. People should generally be able to set limits on how far the public may see into their private life. That a person reveals some facts about their private life certainly does not suggest that all aspects of their private life are then open to public attention. But if a person has invited publicity on a particular matter, it may generally be less reasonable for them to later say that the defendant went too far.

---

65 Arts Law Centre of Australia, *Submission 43*. See, also, Public Interest Advocacy Centre, *Submission 105*.

66 Australian Privacy Foundation, *Submission 110*.

67 '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).

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

6.76 A claim to privacy may also be more difficult to maintain where the plaintiff has been deceptive or hypocritical about the particular matter. Guardian News and Media Limited and Guardian Australia submitted that

> a public figure who makes a public stand on a particular issue may then, inconsistently, seek to cloak particular facts relating to that issue in privacy: in such circumstances the Court should be entitled to consider those additional circumstances. Further it is often the case that plaintiffs' actual conduct can differ from and be inconsistent with their publicly stated views.[69]

6.77 On this last point, it is interesting to compare the comments of Professor James Griffin, in his article *The Human Right to Privacy*:

> a society is the healthier for combating certain forms of hypocrisy; it is certainly better for combating injustice. But a homosexual bishop who believes, even if misguidedly, that priests should not be active homosexuals is not necessarily abusing his power. Not all persons whose appearance differs from their reality are thereby hypocrites. A homophobe, whether homosexual or not, who acts hostilely towards homosexuals solely because they are homosexual is unjust. The injustice deserves exposure. *That* is the public interest. But if the homophobe is himself also homosexual, to publicize that further fact is protected neither by the outer's freedom of expression not the public's right to information. On the contrary, it is an outrageous infringement of the homophobe's right to privacy. It is not that a person's sex life is never of public interest but that usually it is not.[70]

6.78 Other conduct of the plaintiff may strengthen a plaintiff's claim that they had a reasonable expectation of privacy. Notably, it is more reasonable to expect privacy, if one has asked for it. 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. Accordingly, the ALRC recommends that the Act refer to whether, and if so to what extent, the plaintiff had manifested a desire for privacy, in the list of relevant considerations. It was submitted that whether the plaintiff had been 'directly informed about how to manifest a desire not to have his or her privacy invaded' might also be relevant.[71]

6.79 The Australian Privacy Foundation (APF) said there was 'little utility' in this factor. A person should not 'need to express a desire not to be the subject of a tortious wrong'. The APF said that this factor is 'likely to be used by defendants who may use the lack of a demonstrated, overt desire as being a factor to be taken into account against a plaintiff'.[72] The ALRC agrees that a person should not easily be taken to have forfeited their privacy, simply because they did not manifest a clear desire for privacy. But where such a desire for privacy is made manifest, it does seem more reasonable to expect privacy.

---

69 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

70 James Griffin, 'The Human Right to Privacy' (2007) 44 *San Diego Law Review* 697, 720.

71 S Higgins, *Submission 82*.

72 Australian Privacy Foundation, *Submission 110*. Telstra also submitted that whether someone has a manifest a desire not to have their privacy invaded is not relevant: Telstra, *Submission 107*.

Other matters

6.80 The list of factors is not exhaustive. A court may consider other matters when determining whether a person in the plaintiff's position would have a reasonable expectation of privacy.

6.81 For example, the nature of the relationship between the parties may also be relevant. There do not appear to be many cases in which a person has brought an action for invasion of privacy against his or her spouse, partner or other family member. It would generally not be reasonable to expect the same level of privacy from partners and family members. But when relationships break down, the expectation of privacy may then increase. In some cases, the expectation of privacy may even be higher with respect to a former intimate partner, than with others. Women's Legal Services NSW submitted that it is reasonable that victims of family violence should have a higher expectation of privacy.[73]

6.82 Butler submitted a list of matters that should be considered. Many of these matters are included in the list recommended by the ALRC, but others include the intimacy of a sexual relationship; whether the disclosure would cause a risk of serious injury to the plaintiff; and whether the information is 'contained in a public record which is part of the public consciousness'.[74]

6.83 It is not possible to list or analyse all of the factors that may affect whether a person in a particular case can reasonably expect privacy. This is why it is important that a list of relevant factors be non-exhaustive. A court should consider any other relevant factors. By adopting the widely used test of whether the plaintiff had a reasonable expectation of privacy, Australian courts may also draw on the analysis of courts in other countries.

---

73 Women's Legal Services NSW, *Submission 115*.
74 D Butler, *Submission 10*.

7. Fault

Contents

Summary 109
Intentional or reckless invasions of privacy 110
Recklessness 114
What conduct must the fault relate to? 115
Intend the harm? 116
Fault and actionability per se 117
Negligence 118
Strict liability 124
Effect of apology on liability 128

Summary

7.1 There are essentially three types of liability to consider when designing a cause of action for serious invasion of privacy: liability based on intention; liability based on negligence; and strict liability.

7.2 The ALRC recommends that, for an action under the tort to succeed, the invasion of privacy must be either intentional or reckless. Confining the tort in this way will ensure that the new tort applies to the most objectionable types of invasion of privacy.

7.3 Analogous torts protecting fundamental personal rights, such as assault and false imprisonment, also require proof of intent.

7.4 In addition, confining the tort to intentional or reckless conduct is critical to the justification for the tort being actionable without proof of damage. Not requiring proof of actual damage—essentially, allowing actions where there is 'only' emotional distress—will provide an important level of protection and vindication for victims of intentional or reckless invasions of privacy, and will enhance the tort's deterrent and normative influence.

7.5 The cause of action should not extend to negligent invasions of privacy, and should not attract strict liability. Negligence or strict liability would make the scope of the tort too broad.

7.6 This chapter also recommends that an apology should not be admissible as evidence of an admission of fault or liability.

Intentional or reckless invasions of privacy

Recommendation 7–1 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.

7.7 The ALRC recommends that, in a cause of action for serious invasion of privacy, the defendant must be shown to have intended to invade the privacy of the plaintiff. This intention could encompass either:

- a subjective desire or purpose to intrude or to misuse or disclose the plaintiff's private information; or
- circumstances where such an intent may be imputed to the defendant on the basis that the relevant consequences—the intrusion, misuse or disclosure—were, objectively assessed, obviously or substantially certain to follow.

7.8 This approach to intent is consistent with the principles set out in *Fleming's Law of Torts* in relation to the tort of battery,[1] and with the *Restatement (Third) of Torts: Liability for Physical & Emotional Harm.*[2] As discussed further below, the defendant should also be liable if they were reckless.

7.9 It may be helpful for both intent and recklessness to be defined in the legislation. A definition of intent—including both subjective and imputed intent—could be modelled on the US Restatement definition, discussed below. The *Commonwealth Criminal Code* set out in the Schedule to the *Criminal Code Act 1995* (Cth) contains a definition of recklessness that could serve as a model for a definition of recklessness in the new tort. Alternatively, the provision could state that a person is reckless if they are aware of a substantial risk that an invasion of privacy will occur, and acts regardless of, or with indifference to, that risk.

7.10 Previous law reform reports have diverged on the issue of fault. In 2008, the ALRC recommended that liability for invasions of privacy should be limited to intentional or reckless conduct, with 'intentional' defined as being where the defendant 'deliberately or wilfully invades the plaintiff's privacy' and 'reckless' having the same meaning as in s 5.4 of the *Criminal Code* (Cth).[3] The ALRC said that 'including

1 'Battery is an intentional wrong: the offensive contact must have been desired, expected or known to be substantially certain to result': Carolyn Sappideen and Prue Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) [2.60].

2 'Section 1 provides a new general definition of intent. An "intent" to produce a consequence means either the purpose to produce that consequence or the knowledge that the consequence is substantially certain to result': Kenneth W Simons, 'A Restatement (Third) of Intentional Torts?' (2006) 48 *Arizona Law Review* 1061.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) 2576. This report also cited in support: Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy*, (2004) [6.71].

liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[4]

7.11 Neither the New South Wales Law Reform Commission (NSWLRC) nor the Victorian Law Reform Commission (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*.[5] The NSWLRC explained why it had not suggested a fault element in its design:

> We prefer not to lay down an absolute rule [as to whether conduct must be intentional (that is, deliberate or wilful)]. Submissions generally favoured extending liability beyond intentional conduct. While our view is that liability will generally arise under the legislation only where the defendant has acted intentionally there may be circumstances where the defendant ought to be liable for an invasion of privacy that is, for example, reckless or negligent, as where a doctor is grossly negligent in disclosing the medical records of a patient. This is a matter that is appropriately left to development in case law.[6]

7.12 Many stakeholders agreed that the cause of action should be confined to intentional or reckless invasions of privacy.[7]

7.13 Some stakeholders suggested that requiring the plaintiff to prove intent or recklessness sets too high a bar for liability or is too difficult for plaintiffs.[8] However, although the burden of proving fault will be on the plaintiff,[9] it will not always be difficult for the plaintiff to prove that the defendant's conduct involves the first kind of intent above—that is, a subjective desire or purpose. A subjective intent may be obvious on the facts or readily inferred from the defendant's behaviour or statements.

7.14 The second kind of intent—one where the defendant is taken to have intended to invade the plaintiff's privacy—could be described as an 'imputed intent'.[10] In the ALRC's view, the notion of 'imputed intent' is consistent with the well-accepted principle that a person who acts with knowledge of a substantial certainty of a

---

4 ALRC, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 2577. See also NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 171.

5 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.9].

6 Ibid [5.56].

7 ASTRA, *Submission 99*; ABC, *Submission 93*; Australian Bankers' Association, *Submission 84*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; SBS, *Submission 59*; Google, *Submission 54*; Arts Law Centre of Australia, *Submission 43*.

8 Electronic Frontiers Australia *Submission 118*; Public Interest Advocacy Centre, *Submission 105*.

9 The ALRC considers that any statutory action should follow the basic principle that whoever asserts something should bear the onus of proving it: James Goudkamp, *Tort Law Defences* (Hart Publishing, 2013) 12. The ALRC does not consider that a statutory cause of action should follow the unusual, and contentious, position in relation to trespass off the highway that the onus of proving *lack* of fault should be on the defendant: see further Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) 25–27.

10 It was such an imputed intent that Wright J found in the well-known case of *Wilkinson v Downton* when he said: 'It is difficult to imagine that such a statement, made suddenly and with apparent seriousness, could fail to produce grave effects under the circumstances upon any but an exceptionally indifferent person, and therefore an intention to produce such an effect must be imputed': *Wilkinson v Downton* (1897) 2 QB 57, 59. In this case, the defendant had, as a 'practical joke', told the plaintiff that her husband had been badly injured and needed her to collect him in a horse and cab. Mrs Wilkinson suffered a psychiatric illness as a result.

consequence will be *taken* to have intended that consequence. 'Imputed intent' is a short-hand term for this method of finding intent.

7.15 Therefore, a plaintiff would not necessarily have to prove that the defendant had a subjective intent (or purpose) to invade his or her privacy. An intent may be imputed from the circumstances: 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.

7.16 There is little argument against the proposition that, if a statutory tort of invasion of privacy is to be enacted (or a common law tort developed), it should be actionable where the defendant has intentionally invaded the privacy of the plaintiff. Deliberate and unjustifiable invasions of an individual's privacy[11] are clearly culpable and beyond what any person should be expected to endure in the ordinary circumstances and exigencies of everyday life[12] or from their interactions with others in society.

7.17 Protection against intentional or reckless conduct is clearly within the protection intended by art 17 the *International Covenant on Civil and Political Rights*, which provides that*:* 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'. Intentional or reckless invasions of privacy would be likely to be considered 'arbitrary interferences' for the purposes of art 17.

7.18 It is sometimes said that the purpose of a tort is to remedy the *harm* that is suffered by a plaintiff, and that the harm in an invasion of privacy is the interference with the plaintiff's dignity and autonomy, regardless of the type of conduct that causes that interference. However, it can also be argued that the purpose of a tort or statutory action is to remedy and prevent the *wrong* which the plaintiff suffers or may suffer, and that the nature of the conduct and the purpose or motives or state of mind of the actor are closely bound up with making that conduct wrongful.[13] 'Intentional wrongdoers are the worst type of tortfeasor, worse than merely reckless or negligent actors.'[14] This notion is also reflected in the 'seriousness' element, discussed in Chapter 8.

7.19 Most jurisdictions that have a tort or torts of invasion of privacy require that the conduct be intentional or reckless. The statutory torts in four Canadian provinces—British Columbia, Saskatchewan, Newfoundland and Labrador—all apply to a violation of privacy done 'wilfully'.[15] These statutory offences for violation of another's privacy do not distinguish between different types of conduct or invasion.

---

11 That is, assuming that the requirement that there exists a reasonable expectation of privacy has been met.

12 Lord Goff enunciated a similar principle in relation to when a touching in the course of daily life will or will not amount to the tort of battery, in the case of *Collins v Wilcock* (1984) 1 WLR 1172.

13 That the 'mere touching of another in anger is a battery': *Cole v Turner* (1704) 6 Mod Rep 149. Anger or ill intent may turn what would otherwise be an everyday contact into a battery, while hostility is no longer *required* for touching to amount to battery: *Rixon v Star City Pty Ltd* (2001) 53 NSWLR 98, 112.

14 Simons, above n 2, 1079. The author does, however, go on to show how this simple hierarchy of fault is not the whole picture.

15 *Privacy Act*, RSBC 1996, c 373 (British Columbia) s 1(1); *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador) s 3(1); *Privacy Act*, RSS 1978, c P-24 (Saskatchewan) s 2. Only Manitoba uses a different formulation which is that a person 'substantially, unreasonably and without a claim of

7.20 Torts of intrusion upon seclusion in other jurisdictions generally require intentional or reckless conduct. In the American Law Institute's *Restatement (Second) of Tort* (1977), which identifies four privacy torts,[16] only the formulation of the tort of 'intrusion upon seclusion', at s 652B includes the element of intention:

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

7.21 In 2012, the Ontario Supreme Court adopted the elements set out in the *Restatement (Second) of Tort*, to recognise a common law tort of intrusion. Sharpe JA, with whom Winkler CJO and Cunningham ACJ agreed, noted:

> the defendant's conduct must be intentional, within which I would include reckless... A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy.[17]

7.22 Similarly, 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'.[18]

7.23 The *Restatement (Second) of Tort* also identifies a tort relating to giving publicity to a matter concerning the private life of another person, in s 652D. There is no express reference in this tort to fault on the part of the actor.[19]

7.24 The ALRC considers that fault should be required for cases of invasion of privacy involving publication of private information. Intentional—or deliberate—or reckless publications are the primary mischief to which the tort should be directed, and there currently exists a gap in legal protection for such invasions of privacy. While fault is not a distinct element in the torts relating to invasion of privacy by wrongful use or disclosure of private information in other jurisdictions, most have involved deliberate disclosures,[20] either by the media or by individuals formerly in a personal relationship. Fault is rarely at issue, as the defendant's intent to publish or communicate the information about the plaintiff has been obvious. For example, in *Hosking v Runting*, the publication of a photograph of the plaintiff's infant children by the defendants, a photographer and media company, was clearly deliberate.

---

right' violating the privacy of another, but then includes a defence that the defendant neither knew or should have known that the conduct would have violated the privacy: *Privacy Act*, CCSM 1996, c P125 (Manitoba) ss 2(1), 5(1)(b).

16 See Ch 5.

17 *Jones v Tsige* (2012) ONCA 32, [71]–[72]. The ALRC's recommendation on a threshold of seriousness in Ch 8 reflects the criterion of the invasion being 'significant'.

18 *C v Holland* [2012] 3 NZLR 672 ,[94]–[95] (Whata J).

19 The same formulation was adopted by the New Zealand Court of Appeal when it recognised a tort of invasion of privacy by publication of private information: *Hosking v Runting* (2005) 1 NZLR 1, [117] (Gault and Blanchard JJ), [259] (Tipping J).

20 K Barker, *Submission 126*.

7.25 Some stakeholders have suggested that the ALRC should distinguish between the fault required for intrusions upon seclusion and the fault required for wrongful use or disclosure of private information.[21] Others have argued that differing fault requirements for different kinds of invasions of privacy justify having two separate torts.[22] However, conduct invading privacy will often involve both types of invasion and the ALRC considers that the creation of two separate statutory torts would be undesirable. Further, for the reasons set out below, the ALRC considers that any liability under the new tort should be confined to intentional or reckless conduct, regardless of the type of invasion.

7.26 Data breaches caused by or contributed to by negligent conduct, omissions or poor security systems are discussed below. In most cases, if within the jurisdiction, they will attract significant regulatory consequences, which may now include civil penalties, and will give rise to a range of other legal remedies.

Recklessness

7.27 It is the ALRC's view that liability should be extended to situations where the defendant's conduct invaded the plaintiff's privacy recklessly: that is, where the defendant was aware of the *risk* of an invasion of privacy and was indifferent to whether or not an invasion of the plaintiff's privacy would occur as a result of the conduct.[23]

7.28 Recklessness may be described as reckless indifference to a result. In a case involving workplace bullying and harassment, Spigelman CJ said:

> Clearly something substantially more certain [than reasonable foreseeability] is required for the intentional tort ... However, a test of reckless indifference to a result will, in this context, satisfy the requirement of intention.[24]

7.29 Many stakeholders supported the proposal that fault should include recklessness.[25] However, some stakeholders opposed this. For example, Free TV submitted that:

> News and current affairs reporting takes place under strict time constraints that require rapid evaluation of material. In these circumstances, penalties for reckless

---

21 Ibid.

22 Ibid.

23 Recklessness therefore looks to the subjective awareness of the *risk* of an invasion, whereas an imputed intention rests on the obvious or substantial certainty that the invasion would occur.

24 *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417, [76]–[80]. While this statement seems to equate or subsume recklessness within intention, the ALRC considers it clearer to treat recklessness as a separate type of fault from subjective or imputed intention. Note also *Northern Territory v Mengel* (1995) 185 CLR 307, [60]: 'Principle suggests that misfeasance in public office is a counterpart to, and should be confined in the same way as, those torts which impose liability on private individuals for the intentional infliction of harm. For present purposes, we include in that concept acts which are calculated in the ordinary course to cause harm, as in *Wilkinson v Downton*, or which are done with reckless indifference to the harm that is likely to ensue, as is the case where a person, having recklessly ignored the means of ascertaining the existence of a contract, acts in a way that procures its breach.'

25 Insurance Council of Australia, *Submission 102*; ASTRA, *Submission 99*; ABC, *Submission 93*; Australian Bankers' Association, *Submission 84*; SBS, *Submission 59*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*.

> breaches would be likely to introduce a level of conservatism that may prevent or delay the reporting of news, because the test for 'recklessness' in law carries with it a necessary value judgment about what is a reasonable or unreasonable risk.[26]

7.30 The ALRC agrees that there are important public interest considerations involved here. The new tort addresses these concerns by providing that the public interest in the reporting of news on matters of public importance and concern is a matter that a court may take into account, when determining whether there has been an actionable invasion of privacy.[27] These considerations are not best addressed by excluding any liability for reckless conduct.

What conduct must the fault relate to?

7.31 The ALRC considers that the new tort should only be actionable where the defendant intended to invade the plaintiff's privacy in one of the ways set out in the legislation or was reckless as to that invasion. It should not be actionable where there is merely an intention to do an act that has the consequence of invading a person's privacy. In some cases, this distinction will be difficult to draw, such that the consequences of an act will be so inextricably linked to the act, or so substantially certain to follow,[28] 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.

7.32 For example, if an absent-minded person walks into a neighbour's home, thinking it is their own home, the person may have invaded the neighbour's privacy. The action in walking through the front door may have been intended,[29] but the invasion of the neighbour's privacy was not. It would merely have been done negligently.

7.33 To take a more common example, a media entity may publish a story that has the effect of invading a person's privacy, but without any knowledge of the facts which would make it an invasion of that person's privacy.[30] An example would be interviewing a person about the fact that they were adopted as a baby: unknown to the journalist, the person's adoptive parents had not disclosed to their friends the fact that they had adopted their baby. The *publishing* of the story may have been intended, but not the consequences of the publication, namely, the invasion of the parents' privacy by the publication of this information.

7.34 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

---

26 Free TV, *Submission 109*.
27 See Ch 9.
28 Sappideen and Vines, above n 1, 34.
29 Ibid 88.
30 As explained below, lack of knowledge of the facts that make the statement defamatory would not be an excuse to the strict liability under that tort.

of the plaintiff.[31] While Telstra considered current privacy protections sufficient, it submitted that, 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.[32]

7.35 There is much confusion over the use of the term 'intention'. However, some points may clarify the ALRC's recommendation. The requirement does *not* mean that the defendant needs to intend to commit a legal wrong, or that he or she intends to fulfil the other ingredients for liability (seriousness, lack of public interest justification or defence). This would be too stringent a hurdle for the plaintiff to overcome.[33] It does mean that the defendant needs to have been aware of the facts from which it can be objectively assessed whether or not the plaintiff had a reasonable expectation of privacy and of the facts that an intrusion or disclosure would (or in the case of recklessness, may) occur.

7.36 Two examples may explain this last point. First, in relation to private information: some information is obviously private so that there would be no doubt that the defendant would have knowledge of the facts that support a reasonable expectation of privacy. For example, secretly filming a person in the shower, as in *C v Holland*,[34] or surreptitiously prying into someone's bank account, as in *Jones v Tsige*.[35]

7.37 However, in other cases, the defendant may have no knowledge of the facts that would make the disclosure an invasion of privacy. An example is a photographer who takes a photograph of a public event, without realising that the photograph captures a private activity, perhaps of people inside a building in the background to the event. The taking of the photograph in that case would not be an intentional or reckless intrusion into the privacy of the people involved.

Intend the harm?

7.38 Some may argue that requiring an intent to intrude into space or affairs that are private, or disclose information that is private, will remove liability for some conduct that results in a serious invasion of privacy. However, if it were sufficient merely to intend the act, and not the consequences of the act—being the invasion of privacy—then this would effectively impose either a negligence standard (in the sense that the defendant *ought* to have realised the invasion would occur and taken care that it not do so) or a strict liability standard as in defamation. In defamation, the publisher will be strictly liable if the publication defames the plaintiff, even if the defendant was unaware of the facts making it defamatory,[36] or even of the plaintiff's existence or

---

31 See, eg, SBS, *Submission 59*; Telstra, *Submission 45*; Arts Law Centre of Australia, Submission No 15 to DPM&C Issues Paper, 2011.
32 Telstra, *Submission 45*.
33 N Witzleb, *Submission 116*.
34 *C v Holland* [2012] 3 NZLR 672.
35 *Jones v Tsige* (2012) ONCA 32.
36 *Cassidy v Daily Mirror* [1929] KB 331; *Lee v Wilson* (1934) 51 CLR 276.

circumstances.[37] For reasons discussed below, 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.

7.39 It is also clear, by reference to the existing law on other intentional torts, that if the defendant intended the invasion of privacy (that is, to intrude upon the plaintiff's seclusion or to disclose private information), it would *not* be necessary, in order to prove intent, for the plaintiff to show that the defendant intended to offend, distress or harm the plaintiff by the conduct.[38] In an analogous tort, the tort of battery, the tort is made out by proof of an intent to touch, without the need to show an intent to inflict the actual personal injury that followed.[39] 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.[40]

7.40 In some cases, a person will have intent to inflict harm or cause distress to the plaintiff. In such cases, this may satisfy the intent element for the tort,[41] but also amount to 'malice' in law that would aggravate the damages that could be claimed.[42] However, many invasions of privacy will not be motivated by malice towards the victim. If a media organisation invades a person's privacy, this may largely be motivated by a desire to inform the public, pursue a newsworthy story, attract more viewers or increase the sale of newspapers, rather than to harm the victim.

Fault and actionability per se

7.41 If the tort were not confined to intentional or reckless invasions of privacy, but was extended to include negligence or provide for strict liability, this would undermine an important justification for making the tort actionable without proof of damage. Rather, such an extension would require proof of actual damage to be consistent with other tort law.

---

37 *Hulton v Jones* [1910] AC 20; *Mirror Newspapers Ltd v Fitzpatrick* (1984) 1 NSWLR 643. It is only if the fact of publication itself was accidental or could not have been foreseen that a defendant may escape liability: Sappideen and Vines, above n 1, 631. See also, Anthony Dugdale and Michael Jones (eds), *Clerk and Lindsell on Torts* (Sweet & Maxwell, Limited, 19th ed, 2006) 1311–1312.

38 This is described by Simons as a 'dual intent', required by courts in many states of the United States for battery, but he prefers as 'the only plausible interpretation of the case law', the 'single intent' requirement favoured by courts in other states: Simons, above n 2, 1067.

39 What injuries or damage flowing from the tort may be compensated in an intentional tort action is governed by the principles of remoteness of damage: whether the particular head of damage is a natural and probable result of the conduct: *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417, [81].

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

41 'If the only motive of the actor is a desire to harm the plaintiff, this fact becomes a very important factor. A motive of this sort is sometimes called a disinterested malevolence, to indicate that the defendant has no interests of his own to promote by his conduct, other than venting his ill will. It is sometimes said that an evil motive cannot make tortious an act that is otherwise rightful. The nature of the motive, however, may be a factor that tips the scale in determining whether the liability should be imposed or not': American Law Institute, *Restatement of the Law of Torts (Second)* (1977) s 870.

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

7.42 It is not just the law of negligence that requires proof of actual damage. Usually the isolated remaining common law tort causes of action imposing strict liability also require damage, as in the case of liability for nuisance arising out of a positive conduct creating a nuisance.[43] Statutory strict liabilities, such as civil liability to pay compensation for misleading or deceptive conduct, or civil liability in relation to defective products, also only arise where the plaintiff proves loss.[44]

7.43 Defamation liability, which is strict, is a special case. It is actionable per se: there is no requirement that the plaintiff suffer 'actual' or 'special', that is, provable damage. However, it works slightly differently in that a *presumption* of 'general' damage to reputation is inherent in the tort itself.[45]

7.44 Overall, defamation is not a tort the ALRC considers should be used as a model for liability for invasions of privacy, even though some of its elements and defences provide a useful point of comparison. Although there will be no presumption of general damage where the new tort of invasion of privacy is made out—it will be for the plaintiff to persuade the court what emotional distress or other harm they have suffered—the ALRC considers that the combination of strict liability and actionability per se for a new tort of invasion of privacy would still be undesirably onerous on many organisations and individuals.

Negligence

7.45 The ALRC does not recommend that negligent invasion of privacy be actionable under the new tort. Negligence depends on whether the actor's conduct[46] 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. In this objective test, the intention of the defendant is not relevant, even if the defendant was well-meaning.[47]

7.46 A number of stakeholders submitted that liability for breach of privacy should be imposed for negligent invasions of privacy, in addition to reckless and intentional invasions of privacy.[48] As noted above, however, many stakeholders submitted or

---

43 Sappideen and Vines, above n 1, 509.

44 See, eg, *Competition and Consumer Act 2010* (Cth) sch 2.

45 '[Special damages] are much less important than general damages, which are presumed to follow publication of the libel. The claimant does not have to prove the particular respects in which it has damaged his reputation or injured his feelings.': Eric Barendt et al, *Media Law: Text, Cases and Materials* (Pearson, 2013) 445; Sappideen and Vines, above n 1, 632–634. See also *Defamation Act 2005* (NSW) 2005 s 7(2).There are equivalent provisions in the other Australian uniform defamation laws which provide that 'the publication of defamatory matter of any kind is actionable without proof of *special* damage'. 'Special damage' refers to particular financial loss which the plaintiff proves was caused by the tort, such as cancellation of a sponsorship contract or loss of profits. See, also, Ch 8 and *Ell v Milne (No 8)* [2014] NSWSC 175 (7 March 2014).

46 In this context, 'conduct' might be comprised of an omission to do something. It could also refer to the actor's conduct in operating or maintaining a system, such as a data storage system.

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

48 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*.

argued strongly that the requisite fault should not extend to negligence. Some argued that fault should be relevant only to damages, or that reasonable care should be a defence.[49]

7.47 There were two main arguments for extending liability to negligence: first the harm that may result from negligence; secondly, the deterrent or regulatory effect of negligence liability.

Harm caused by negligence

7.48 Some stakeholders who called for negligence-based liability stressed the harm that may be caused by unintentional invasions of privacy,[50] arguing that negligence can be just as damaging as, or even more damaging than, intentional or reckless conduct.[51]

7.49 Two possible types of harm need to be distinguished. First, where 'actual damage'—in the form of physical injury, psychiatric illness, property damage or financial loss—has been suffered by the plaintiff from the defendant's negligent invasion of privacy; and secondly, where the harm to the plaintiff is emotional distress only.

7.50 The first kind of harm may already be actionable under existing law. The ALRC considers that, because of this, the new cause of action should not extend to cover such situations. As the ALRC pointed out in the Discussion Paper, if actual damage is suffered beyond 'mere' emotional distress, it may well be the case that the plaintiff would already have a tort action in negligence because the defendant would be under a duty of care to the plaintiff.

7.51 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 straightforward to succeed in a negligence claim where a plaintiff has suffered physical injury or property damage due to another's negligence. If the harm is in the form of psychiatric illness, civil liability statutes in most states and territories impose extra requirements for recovery.[52] If the claim is for pure economic loss, then the requirements for liability are specific, but Australian courts do recognise such claims in limited circumstances. Much will depend on whether the defendant knew of the plaintiff and the risk of financial loss to that plaintiff, whether the defendant had made a representation to the plaintiff and whether the plaintiff was able to protect themself from the effects of the defendant's negligence.[53]

---

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

50 See, 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*.

51 Electronic Frontiers Australia *Submission 118*.

52 See, eg, *Civil Liability Act 2002* (NSW) pt 3.

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

7.52 This kind of negligence may occur in the privacy context in situations involving data breaches. In many cases of data breach, the parties are already known to each other through a series of transactions or contractual or licensing arrangements—the plaintiff may, for example, be a customer of the defendant.

7.53 In addition, or alternatively to tort liability, the plaintiff who has suffered actual loss as a result of a negligent data breach is likely in many cases to have a claim for breach of contract. It would not, it is suggested, be difficult to find an implied term that private information about the plaintiff should not be disclosed except for the purposes of the contract or in compliance with terms of the contract. Liability in contract may be strict or negligence-based. In addition, the plaintiff may also have a claim under the Australian Consumer Law or an equitable claim for breach of confidence, if the information was collected in confidence, as would often be the case.

7.54 In the second, and probably more common,[54] type of scenario, where the plaintiff has suffered only emotional distress, negligence liability would provide no remedy, nor would consumer protection laws. Contract law will only remedy mental distress when protection or freedom from such distress is a major or important purpose of the contract.[55] Compensation for distress may be awarded in appropriate contractual breach of confidence cases.[56]

7.55 Negligence law would provide no remedy, because the well-entrenched policy of the common law—and now the clear legislative policy across most Australian states and territories—is that liability for negligence generally does not extend to 'mere' emotional distress.[57] PIAC argued that this is not a convincing reason of principle as to why liability for invasion of privacy should not do so, as 'the nature of the breach is distinct and the facts are commonly if not invariably different from those involved in other forms of negligence'.[58] The Australian Privacy Foundation also argued that the new tort 'is discrete and stands alone, being designed to address specific forms of harm'.[59]

7.56 However, there are very many distressing situations in society caused by another's negligence, yet recovery is denied. If the new tort were to provide both that it should be actionable per se or should treat emotional distress as actual damage *and* that fault should extend to negligence, the coherence and overall consistency of the law in Australia would be undermined. Not only would the proposal conflict with clear legislative policy, but it is also difficult to see, as a matter of fairness, why a person should be able to recover for emotional distress caused by a negligent but unintentional invasion of privacy when another can recover nothing for emotional distress in a wide range of situations: the loss of a child's or other family member's life due to the

54 Leaving aside the common problem of fraud and identity theft where the plaintiff suffers actual financial loss.

55 *Farley v Skinner* (2002) 2 AC 750, 755; John W Carter, *Contract Law in Australia* (Lexis Nexis Butterworths, 6th ed, 2013) 855.

56 *Cornelius v de Taranto* [2001] EMLR 12, [69].

57 See, eg, *Civil Liability Act 2002* (NSW) s 31.

58 Public Interest Advocacy Centre, *Submission 105*.

59 Australian Privacy Foundation, *Submission 110*.

negligence of another person; from closely witnessing a terrifying event caused by negligence; or even from malicious conduct specifically aimed at distressing the plaintiff.[60]

7.57 Some stakeholders submitted that it would be consistent with the tort of 'negligent trespass', which is still recognised in Australia,[61] if a tort of invasion of privacy was actionable per se even where committed negligently.[62] However, the analogy is arguably inapt. While there are many case authorities, including in the High Court of Australia, which support an action of negligent trespass for direct physical impact and injury,[63] there is no case authority which supports the view that a trespass comprising an assault or false imprisonment and without any physical damage is actionable as a trespass (per se) on the basis of negligence. In fact there are numerous cases which analyse the requirement of intention in assault cases and whether intention was made out on the facts.[64] The ALRC suggests that the correct view is that assault and false imprisonment—and their actionability per se—are torts of intention or recklessness. Being concerned with intangible and dignitary interests of the plaintiff, these are the torts that are most analogous to an invasion of privacy.[65]

Deterrence and regulation

7.58 The second main argument advanced by stakeholders for extending liability to negligence, was the potential deterrent or regulatory effect of liability. Excluding negligence, it was argued, would encourage indifference to invasions of privacy.[66] 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

---

60 As in the United Kingdom, there is no tort in Australia of intentionally causing 'mere', even severe, emotional distress.

61 Unlike in England since the Court of Appeal decision of *Letang v Cooper* (1965) in which Lord Denning limited actions in trespass to intentional wrongs. This decision has been criticised in Australia: *NSW v Knight* [2002] NSWCA 393. This decision has also been criticised in the United Kingdom. See Ulele Burnham, 'Negligent False Imprisonment—Scope for Re-Emergence?' (1998) 61 *Modern Law Review* 573. But the real problem identified in that article seems to be not that a tort of false imprisonment cannot be brought on the basis of trespass if negligently committed, but that it is not clear if mere detention is to be treated as actual damage for the purposes of a negligence action. Further, in England, there is the difficulty of suing public authorities in negligence.

62 N Witzleb, *Submission 116*.

63 *Williams v Milotin* (1957) 97 CLR 465, 474.

64 Sappideen and Vines, above n 1, 35. Kit Barker et al, *The Law of Torts in Australia* (Oxford University Press, 2012) 46. Cf Balkin and Davis, above n 9, 41. Luntz et al, notes the lack of case authority for the proposition that there can be a 'negligent assault': Harold Luntz et al, *Torts: Cases and Commentary* (Lexis Nexis Butterworths, 7th ed, 2013) 621. Lord Hope defined assault as 'any act by which the defendant, intentionally or recklessly, causes the claimant to apprehend immediate and unlawful personal violence', noting that 'this meaning is well vouched by authority': *R v Ireland* [1997] 4 All ER 255.

65 The same may well be true of battery, leaving the generic term 'negligent trespass' to apply only to negligent, direct, unauthorised, physical contact. Barker et al argue against the continuing role of negligent trespass. Barker et al, above n 64, 34. In *Marion's Case*, McHugh J described battery as follows: 'The essential element of the tort is an intentional or reckless, direct act of the defendant which makes or has the effect of causing contact with the body of the plaintiff': *Marion's Case* (1992) 175 CLR 218, 311.

66 Law Institute of Victoria, *Submission 22*.

breaches.[67] Bruce Arnold submitted that the action for negligence 'provides a necessary and appropriate incentive for Australian organisations to move towards best practice in information management'.[68]

7.59 The Law Institute of Victoria argued that '[i]ntentional 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.[69]

7.60 PIAC also suggested that many systemic breaches of privacy may be due to negligence:

> 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.[70]

7.61 However, at least in respect of data breaches by government agencies and organisations with a turnover of more than $3 million, there is already considerable regulation to protect private information. Such entities are required to take such steps under the *Privacy Act* (and to some extent the *Telecommunications Act*), or under state and territory legislation.[71] Although it could be argued that these Acts have significant gaps, due to exemptions for most small businesses, for the media, and for most individuals, the new tort cause of action should not be designed as a remedy for deliberate exemptions in existing legislation. Instead, it may be more appropriate for that legislation to be reviewed, amended or strengthened.

7.62 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 Privacy Commissioner. Since March 2014, this includes the possibility of substantial civil penalties.[72] While the advent of these reforms and new regulatory powers is not a reason, of itself, to stall the introduction of a tort directed at intentional invasions of individual privacy, as argued by some stakeholders,[73] they do counteract the argument that the existing law encourages indifference and negligence in systems maintenance. The ALRC considers that, in general, 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.

---

67 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'.

68 B Arnold, *Submission 28*. See, also, Law Institute of Victoria, *Submission 22*. The Law Institute of Victoria submitted that, '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'.

69 Law Institute of Victoria, *Submission 22*.

70 Public Interest Advocacy Centre, *Submission 30*.

71 See Ch 3.

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

73 Interactive Games and Entertainment Association, *Submission 86*.

Too wide a liability

7.63 If the new tort extended to negligent invasions of privacy, there is a serious potential for a wide range of people to face liability for invading privacy by common human errors. While the ALRC agrees that human error is not synonymous with negligence,[74] and that negligence depends on an objective standard of the reasonable person, nevertheless the law of negligence does not consider degrees of negligence. A small degree of negligence, a momentary lapse of attention, may be adjudged to be negligence, and the extent of the harm is irrelevant to this issue. Further, in a negligence case, the defendant's conduct is also a breach of a pre-existing legal duty owed to the plaintiff or to a class to whom the plaintiff belongs: what may be expected of a defendant depends on the nature and scope of the duty of care. The proposed liability would not depend on a pre-existing duty of care.

7.64 A tort based on negligent invasion of privacy could capture many accidental or unintended occurrences. It is entirely conceivable that many legitimate activities may involve the unintended invasion of the privacy of a person unknown to the defendant. Street photography, CCTV cameras, drone usage or media activities may inadvertently capture footage or images of private activities or intrude into private spheres. Private information may be posted online or disclosed or lost in circumstances that a court could find to be negligent, even though that was done accidentally. If negligence were a basis of liability, it would be open for a plaintiff to argue that the defendant *should* have taken more precautions to ensure that these consequences did not happen.

7.65 It was suggested in the Canadian case, *Jones v Tsige,* that confining the tort to intentional and reckless conduct will help ensure the new tort will not 'open the floodgates' to privacy claims.[75]

7.66 While data breaches by commercial and government entities should be treated seriously by the law, there is a real risk, in the ALRC's view, that extending liability to negligence generally would lead to onerous and broad liability under the new tort, and in view of existing remedies and regulation outlined above, there is no compelling case to so extend it.

Chilling effect of negligence liability

7.67 Some stakeholders argued that extending liability to include negligence might lead people to be 'unduly careful about disclosing information'.[76] It may lead to excessive self-censorship[77] or too great a chilling effect on everyday activities that carry even a remote risk of unintentionally invading someone's privacy. The Arts Law Centre said that it would be concerned

> that creating a cause of action for negligence has the potential to create a great deal of uncertainty and discourage artists from engaging in activities that could accidentally

74 N Witzleb, *Submission 116*.
75 *Jones v Tsige* (2012) ONCA 32, [71]–[72].
76 ASTRA, *Submission 47*.
77 National Association for the Visual Arts Ltd, *Submission 78*.

> or inadvertently expose them to the risk of breaching the law. Inadvertent invasions will lead to self censorship, chilling effect.[78]

7.68 The Australian Privacy Foundation argues that a robust public interest defence, which protects freedom of speech, would obviate problems that negligence liability would chill or inhibit free expression or free speech.[79] However, it is implicit in the assertion of public interest that the conduct was deliberately done *in* the public interest.

Recklessness is a preferable standard to gross negligence

7.69 Some stakeholders, while accepting the argument that negligence may be too wide a liability, argued that 'gross negligence' should be sufficient fault to ground liability. The UNSW Cyberspace Law and Policy Community submitted that

> excluding negligence entirely provides minimal incentive to put in place procedures to protect privacy. The inclusion of a 'gross negligence' standard would provide such incentives, while avoiding liability for the 'absent-minded person' who 'walks into a neighbour's home'.... A gross negligence standard will increase the reach of the proposed tort.[80]

7.70 However, Australian tort law does not recognise a concept of gross negligence[81] and it could be a source of uncertainty.

7.71 In the ALRC's view, the inclusion of recklessness as a form of fault will come close to what some may have in mind when referring to 'gross negligence'. While negligence refers to unreasonable *inadvertence* to a risk, a situation where the actor *ought reasonably* to have foreseen but did not foresee a risk, recklessness refers to a subjective state of mind where the actor was aware of the risk but did not care whether or not it occurred.[82] In many situations involving serious data breaches, for example, the risk may be well-known in the industry so that it may be obvious or provable that the defendant was aware of the risk, providing the basis for a finding of recklessness, or even intent on an imputed basis.

Strict liability

7.72 The ALRC does not support the new tort imposing strict liability. Strict liability leads to liability regardless of fault. If the cause of action were one of strict liability,

---

78 Arts Law Centre of Australia, *Submission 113*.

79 Australian Privacy Foundation, *Submission 110*. See also N Witzleb, *Submission 116*.

80 UNSW Cyberspace Law and Policy Community, *Submission 98*.

81 Sappideen and Vines, above n 1, 148. The criminal law has a standard of criminal negligence which tends to be higher than the civil standard of care in negligence. For example the *Criminal Code Act 1995* (Cth) sch, s 5.5 defines negligence as conduct that involves such a great falling short of reasonable care that the conduct merits criminal punishment.

82 See Lord Millet in *Three Rivers DC v Bank of England (No 3)* about the tort of misfeasance in public office: 'This is an intentional tort. It involves deliberate or reckless wrongdoing. It cannot be committed negligently or inadvertently. Accordingly it is not enough for the [claimants] to establish negligence, or even gross negligence, on the part of the [defendant]. They must establish some intentional or reckless impropriety': *Three Rivers DC v Bank of England (No 3)* [2003] 2 AC 1 [179] (Lord Millet). See also, *Three Rivers DC v Bank of England* [2000] UKHL 33; *Bici v Ministry of Defence* [2004] EWHC 786 (QB).

then the defendant would be held liable even though they were not at fault, that is, the defendant's actions were not intentional, reckless or negligent.

7.73 The ALRC considers that strict liability would be too onerous and broad, and that it is inconsistent with modern trends in tort law to fault-based liability. Examples of statutory strict liability are directed at pecuniary loss or material damage in particular contexts, such as consumer protection or product liability, unlike claims for invasion of privacy which will arise in a wide variety of contexts and generally involve dignitary or intangible interests.

7.74 For similar reasons to those outlined in respect of negligence-based liability, it would not be appropriate to make a strict liability tort actionable per se, yet this feature of the new tort is an important protection of privacy from intentional or reckless invasion.

7.75 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 infliction of harm. That is not a statement of law but a description of the general trend.[83]

7.76 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 ... Does reputation deserve a higher level of protection than personal safety?[84]

7.77 The ALRC considers that the same may be said of privacy.

7.78 The *Uniform Defamation Laws* that came into force in the Australian states and territories in 2006 does provide for a defence of innocent dissemination,[85] so that an absence of fault may excuse the defendant. 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'.[86] Nevertheless, liability arises upon publication.[87] It is not incumbent on the plaintiff to prove that the

---

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

84 Sappideen and Vines, above n 1, 630.

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

86 Ibid s 32(1)(b). This is similar to the position in *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 5(b).

87 The plaintiff must be identifiable from the publication. This may occur even where the plaintiff is not named. See, further, Sappideen and Vines, above n 1, 623.

defendant knew that the publication was defamatory of the plaintiff or even knew the circumstances that rendered the publication defamatory or that the defendant failed to take care in relation to the publication of the statement.[88]

7.79 Liability in defamation is notoriously onerous and is widely regarded as a significant limitation on freedom of speech in Australia,[89] and particularly burdensome on the media,[90] compared to the position in other countries such as the United States and the United Kingdom. The ALRC considers it undesirable to introduce a tort that would lead to a potential liability as onerous and as restrictive on freedom of speech as current liability in defamation.

7.80 Most strict liabilities now arise by statute[91] and provide a remedy for physical damage or financial loss. Important examples in Australian law are:

- statutory liability for (financial) 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*;[92]
- statutory liabilities for physical damage caused by defective products;[93] and
- statutory liability for damage caused by aircraft.[94]

7.81 The Office of the Australian Information Commissioner (OAIC) noted that no fault element is required for complaints made to the OAIC for an interference with privacy under the *Privacy Act*, and that 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'.[95] 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.*

---

88 'Publication' may even be comprised by a failure to remove a publication where there was power to do so: *Byrne v Deane* [1937] 1 KB 818.

89 David Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy' (2012) 17 *Media & Arts Law Review* 170, 195.

90 Australian defamation law does not include a principle such as that in *New York Times v Sullivan*, which requires public figures to show malice in order to sue for libel: *New York Times v Sullivan* [1964] 376 US 254. Nor does Australian defamation law provide for a responsible journalism defence, such as formulated in the UK in *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127. Australian defamation law does not include a wide public interest defence such as in *Defamation Act 2013* (UK) s 4(6).

91 A statute imposing a strict liability may be the basis of a common law tort of breach of statutory duty: Sappideen and Vines, above n 1, 434.

92 *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.

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

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

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

7.82 Some have argued that one reason why liability for invasions of privacy should be strict, at least with respect to wrongful disclosure of private information, is that this would be consistent with actions in defamation and breach of confidence.[96] However, the analogy with breach of confidence 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.[97] There is therefore a stronger case for strict liability in such circumstances than under the new tort where a plaintiff merely has to show a reasonable expectation of privacy.

7.83 Further, given that the ALRC does not recommend that the new tort of invasion of privacy replace the action for breach of confidence, a plaintiff who can rely on a pre-existing obligation of confidence will still be able to sue in that equitable action, relying on strict liability.[98] Such plaintiffs would also, no doubt, wish to rely on the favourable principles underlying the remedy of an injunction in the equitable breach of confidence action.[99]

7.84 Some stakeholders suggested that some invasions of privacy should not attract liability where 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.[100] Similarly, SBS noted:

> 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.[101]

7.85 The Australian Bankers' Association submitted that '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.[102]

7.86 The ALRC agrees that strict liability would be too onerous.

---

96 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; *Cassidy v Daily Mirror* [1929] KB 331. See also K Barker, *Submission 126*.

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

98 See for example, *Candy v Bauer Media Limited* [2013] NSWSC 979 (20 July 2013).

99 See Ch 13.

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

101 SBS, *Submission 59*.

102 Australian Bankers' Association, *Submission 27*.

Effect of apology on liability

Recommendation 7–2 The Act should provide that an apology made by the defendant does not constitute an admission of fault or liability and is not relevant to the determination of fault or liability.

7.87 The ALRC recommends that any apology or correction of published material by a defendant should not be treated in evidence as an admission of fault. [103]

7.88 This recommendation is intended to encourage the early resolution of disputes without recourse to litigation. It is similar to provisions in state and territory legislation regulating civil liability,[104] and in defamation law.[105] There is a body of academic literature supporting the role of apologies in resolving disputes and such provisions as a mechanism for achieving justice between disputants. There was also strong stakeholder support for this proposal.

7.89 The ALRC considers that the definition of apology in the NSW *Civil Liability Act 2002* should apply to this recommendation:

> 'apology' means an expression of sympathy or regret, or of a general sense of benevolence or compassion, in connection with any matter whether or not the apology admits or implies an admission of fault in connection with the matter.[106]

7.90 Apologies are often associated with an assumption or admission of guilt and are therefore seen to be 'highly prejudicial'.[107] This recommendation aims to encourage individuals to make apologies without the risk of liability:

> It would detract from any dispute resolution process of the parties were reluctant to offer an apology due to possible use as evidence of fault or liability.[108]

7.91 Encouraging defendants to make formal apologies may assist with the resolution of disputes as, in many circumstances, an apology may provide a sufficient response to

---

103 Several stakeholders supported this recommendation: Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Telstra, *Submission 107*; Public Interest Advocacy Centre, *Submission 105*; Telecommunications Industry Ombudsman, *Submission 103*; Insurance Council of Australia, *Submission 102*; Australian Bankers' Association, *Submission 84*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; N Witzleb, *Submission 29*.

104 For example, *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; Australian Treasury, 'Review of the Law of Negligence: Final Report' (2002).

105 *Defamation Act 2005* (NSW) 2005 s 20; *Defamation Act 2005* (Qld) 2005 s 20; *Defamation Act 2005* (SA) 2005 s 20; *Defamation Act 2005* (Tas) s 20; *Defamation Act 2005* (Vic) s 20; *Defamation Act 2005* (WA) s 20.

106 *Civil Liability Act 2002* (NSW) s 68.

107 Vines, 'The Apology in Civil Liability: Underused and Undervalued?', above n 104, 30.

108 Telecommunications Industry Ombudsman, *Submission 103*.

appease someone whose privacy has been invaded. Guardian News and Media Limited and Guardian Australia supported this point, arguing that

> Parties should be encouraged to resolve matters prior to or during litigation. The nature of invasions of privacy is that in many instances an apology, freely given, may be sufficient to resolve the matter. Accordingly, protecting the making of apologies is an important aspect of the ALRC's proposals.[109]

7.92 The Telecommunications Industry Ombudsman provided analysis of the positive role apologies play in the resolution of disputes under their complaints model:

> From our experience, consumers will request apologies to resolve privacy complaints and an apology genuinely made has the potential to encourage the early resolution of disputes. It would detract from any dispute resolution process if the parties were reluctant to offer an apology due to possible use as evidence of fault or liability. An apology can be an important part of resolving a dispute and it is one of several readily available remedies used in ADR processes. From our experience, apologies can help:
>
> - diffuse tension and create common ground between opposing parties
> - foster constructive discussion and even conciliation between parties
> - alleviate injury and distress caused to aggrieved parties, and
> - reduce the length and severity of disputes.[110]

7.93 Australian research shows that in medical negligence cases, apologies (not court-ordered apologies), can have psychological benefits to plaintiffs.[111]

7.94 Prior to the enactment of the *Uniform Defamation Laws* in 2005, there was a disincentive for a publisher to apologise for publishing defamatory matter since such an apology could be construed as an admission of liability.[112] Civil liability legislation stipulating that apologies should not be taken as admissions of fault reflects a similar concern:

> It was felt that if people apologise it was less likely that there would be litigation; and there is indeed some evidence for this proposition.[113]

7.95 Dr Ian Turnbull raised the concern that some defendants may use apologies as a vehicle to exacerbate the harm caused by the initial invasion, as publishing an apology may

> reconvey the private information to a wider audience as part of the apology. That is particularly so where media is used and, for example, a more prominent location within the website or paper is used for the apology.[114]

---

109 Guardian News and Media Limited and Guardian Australia, *Submission 80*.
110 Telecommunications Industry Ombudsman, *Submission 103*.
111 Carroll, above n 104, 319.
112 Des A Butler and Sharon Rodrick, *Australian Media Law* (Thomson Reuters (Professional) Australia Limited, 2011) [3.600].
113 Vines, 'The Apology in Civil Liability: Underused and Undervalued?', above n 104, 28.
114 I Turnbull, *Submission 81*.

7.96 To ameliorate this harm, Turnbull suggested the recommendation be qualified by a requirement that the apology be 'sincere' or 'genuine'.[115] The ALRC considers that it is more appropriate to consider the nature or quality of any apology when a court assesses an award of damages.

115 Ibid.

8. Seriousness and Proof of Damage

Contents

Summary 131
Seriousness 132
The need for a threshold 132
Serious 134
Offence, distress and other privacy harms 134
Knowledge and motive of the defendant 137
A higher threshold? 137
Proof of damage not required 138

Summary

8.1 The tort designed in this Report is concerned with providing civil redress for *serious* invasions of privacy. The ALRC recommends that this should be made clear in the Act, by including a separate and discrete element of the tort requiring a court to consider whether the invasion of privacy was 'serious'. This will help deter people from bringing trivial privacy claims before the courts.

8.2 Guidance on the meaning of serious should be provided in the statute. The relevant Act should provide that a court may consider the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause a person of ordinary sensibilities in the position of the plaintiff. The Act should also provide that courts may consider whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff.

8.3 Other matters may also be relevant, but the ALRC considers these to be the most important. Including them will provide some certainty about the meaning of 'serious'.

8.4 The second question discussed in this chapter is whether the plaintiff should be required to prove that they suffered 'actual damage'—more than emotional distress—from the invasion of privacy. Given the invasion of privacy must not only be serious, but the defendant must have invaded the plaintiff's privacy intentionally or recklessly, the ALRC considers the plaintiff should not also have to prove that they suffered actual damage. The tort should be actionable per se.

8.5 Further, in many 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

Recommendation 8–1 The Act should provide that a plaintiff has an action under the new tort only where the invasion of privacy was 'serious', having regard, among other things, to:

(a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff; and

(b) whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff.

The need for a threshold

8.6 Some invasions of privacy should not be actionable, because they are not sufficiently serious. The ALRC recommends that the Act provide for a threshold test of seriousness that would ensure that trivial and other non-serious breaches of privacy are not actionable.

8.7 The *Privacy Act 1988* (Cth) provides for civil penalties in cases of 'serious' or 'repeated' interferences with privacy.[1] A seriousness threshold is also recognised in the United Kingdom (UK). Hon. Justice Roger Toulson and Charles 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'.[2] 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.[3]

8.8 Some stakeholders submitted that there should not be an additional threshold.[4] If a person has a reasonable expectation of privacy then, subject to public interest matters,

---

1 *Privacy Act 1988* (Cth) s 13G. The Act does not define 'serious'; the ordinary meaning of the word applies.

2 Roger Toulson and Charles 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'.

3 *Ambrosiadou v Coward (Rev 1)* [2011] EWCA Civ 409 (12 April 2011) [30] (Lord Neuberger MR).

4 A number of stakeholders opposed an additional separate threshold: eg, N Witzleb, *Submission 116*; Australian Privacy Foundation, *Submission 110*; Public Interest Advocacy Centre, *Submission 105*; 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*.

the person should have an action. It was also suggested that, where there is a reasonable expectation of privacy and no countervailing public interest, then an invasion would necessarily be serious, and therefore an additional threshold unnecessary.

8.9 The Australian Privacy Foundation submitted that an additional threshold for seriousness was 'unnecessary and arbitrary':

> If the cause of action is structured as an intentional tort, as the cause of action appears to be, damage should be presumed. The remedy, whether in the form of injunctive relief, damages or other relief, will (or should) reflect the seriousness of the breach.[5]

8.10 Associate Professor Paul Wragg also had some concerns. Although he said the point should not be overstated, given that the risk would not to arise in obvious cases, there was a 'danger of the seriousness standard being applied twice if not three times':

> first through the 'reasonable expectation of privacy' test where the UK standard (which already excludes non-serious intrusions) is taken as the benchmark; secondly, as a means of limiting interferences to those that not only satisfy the reasonable threshold standard but also may be said to be a serious breach of that standard (so as to be highly offensive, etc) and thirdly (potentially) through the use of the balancing approach where the intrusion must not only be serious but also so serious as to outweigh everyone else's rights (ie, the public interest at stake).[6]

8.11 The New South Wales Law Reform Commission also did not see the need for an additional threshold.[7] There is no threshold of seriousness in the statutes of the four Canadian provinces which have a statutory cause of action for invasion of privacy.[8]

8.12 Some stakeholders, however, submitted that there should be a discrete seriousness threshold.[9] Some suggested that there should be a threshold, but that it should be set at 'highly offensive' invasions of privacy, rather than merely 'serious' ones.[10] Others said that the threshold should be a high one, so that the new tort does not undermine freedom of expression and of the media.[11]

8.13 The ALRC has concluded that there should be an additional threshold of seriousness. In some circumstances, it will be obvious that the invasion of privacy was serious. In fact, the seriousness may well often be evident from the other elements of the offence. If a plaintiff has a reasonable expectation of privacy, and this privacy is

---

5 Australian Privacy Foundation, *Submission 110*.

6 P Wragg, *Submission 73*.

7 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [23]–[33].

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

9 See, eg, Women's Legal Services NSW, *Submission 115*; Office of the Victorian Privacy Commissioner, *Submission 108*; ASTRA, *Submission 99*; ABC, *Submission 93*; Google, *Submission 91*; Australian Bankers' Association, *Submission 84*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; National Association for the Visual Arts Ltd, *Submission 78*; Telstra, *Submission 45* ('A seriousness threshold must be imposed, both in order to discourage trivial or minor claims, and in order to provide business and the community with a level of certainty and consistency in its application').

10 SBS, *Submission 123*; ABC, *Submission 93*.

11 The ALRC recommends a separate public interest balancing test in Ch 9.

intentionally invaded, then in some cases the facts leading to these conclusions will themselves strongly suggest the invasion of privacy was serious. However, an additional and discrete threshold of seriousness would provide an additional means of discouraging people from bringing actions for trivial invasions of privacy. The risk of non-serious actions or a proliferation of claims was raised by a number of stakeholders.[12]

8.14 For similar reasons, a serious harm test has been introduced to defamation law in the UK. The *Defamation Act 2013* (UK) provides that a 'statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant'.[13] This provision was intended to discourage trivial claims.[14]

8.15 The ALRC also considers that a discrete seriousness threshold, in addition to the public interest balancing test,[15] would further ensure the new tort does not unduly burden competing interests such as freedom of speech.

Serious

8.16 If there is a threshold, where should it be set? The ALRC recommends the Act provide that for the plaintiff to have an action, the court must consider the invasion of privacy 'serious'.

8.17 'Serious' can mean 'not trifling', 'weighty or important',[16] 'important, demanding consideration, not to be trifled with, not slight'.[17] These definitions may be helpful, but the ALRC recommends that the Act provide specific guidance to courts on the meaning of serious. This guidance should be in the form of a few important factors for the court to consider, along with any other relevant factor, when determining whether an invasion of privacy was serious. These factors are discussed below.

8.18 This is an objective test. It is not about whether the plaintiff considered the invasion of privacy to be serious, or even whether the plaintiff has proved that they suffered serious damage from the invasion of privacy.[18] Rather, it is about whether the court views the invasion as serious.

Offence, distress and other privacy harms

8.19 The first and perhaps most important factor for a court to consider when determining whether an invasion of privacy was serious is the degree of any offence,

---

12 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.

13 *Defamation Act 2013* (UK) s 1.

14 Jonathan Djanogly MP quoted in James Price (ed) and Felicity McMahon (ed), *Blackstone's Guide to the Defamation Act 2013* (Oxford University Press, 2013) 20. This provision differs from the seriousness test recommended by the ALRC in a few ways. Perhaps most notably, the UK provision is a subjective test—harm or likely harm to the claimant must be proven.

15 See Ch 9.

16 Macquarie Dictionary.

17 Concise Oxford Dictionary.

18 The plaintiff should not be required to prove actual damage: Rec 8–2.

distress or harm to dignity that the invasion of privacy was likely to cause a person of ordinary sensibilities in the position of the plaintiff. This should be set out in the Act.

8.20 Although other harms may often be relevant, offence and distress are two common types of harm that commonly follow serious invasions of privacy.

8.21 Professor Kit Barker submitted that the essence of what is wrong about an invasion of privacy is 'harm to the personal dignity of the plaintiff and/or the plaintiff's autonomy in controlling elements of his or her private life'.[19] The ALRC agrees that these are important types of harm that should be considered by a court in determining whether a particular invasion of privacy was serious.

8.22 The privacy and dignitary interests of a person may be harmed without that person's knowledge. For example, in some circumstances it may 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, or perhaps even of a young child, despite the fact that a person is unlikely to be offended or distressed by the incident or the publication. Such invasions of privacy may be serious, even though distress, offence or harm to the plaintiff may be unlikely. This is one reason why offence and distress are not the only harms that might make an invasion of privacy serious.[20]

Extent of harm

8.23 In the Discussion Paper, the ALRC proposed that courts consider whether the invasion of privacy was likely to be 'highly' offensive, distressing or harmful.[21] This may have suggested that if it were not highly offensive, highly distressing or highly harmful, it could not be serious. As a number of stakeholders pointed out, this may be too limiting.[22] Some offensive, distressing or harmful invasions of privacy will be serious, even when the invasion cannot be described as 'highly' offensive, distressing or harmful.

8.24 The ALRC therefore recommends that a court consider the 'degree' or 'extent' of the offence, distress or harm to dignity likely to be caused by the invasion of privacy. The greater the likely offence, distress or harm, the more likely the invasion will be serious. This formulation provides the court with somewhat more discretion in its assessment of seriousness.

A person of ordinary sensibilities in the position of the plaintiff

8.25 It is important to ask whether the conduct was likely to offend, distress or harm the dignity of a person 'in the position of the plaintiff'. Most people are not particularly

---

19 K Barker, *Submission 126*.

20 'A young child photographed naked through a telephoto lens may well experience no offense or distress at all. Nor is it really relevant whether anyone else is offended by the publication of the photograph. The point is that privacy laws should "carve out some personal space" for the child which protects it against such intrusion and potentially prejudicial disclosure.': Ibid.

21 This was intended to mean 'highly offensive, highly distressing or highly harmful'.

22 'If a seriousness threshold were introduced, it should be set at "offensive, distressing or harmful". I believe that it would be setting the bar much too high if a privacy invasion was actionable only if it was, or was likely to be, "highly distressing" or "highly harmful"': N Witzleb, *Submission 116*.

offended, distressed, much less harmed, when the privacy of other people—particularly strangers—is invaded. The seriousness of an invasion of privacy should not be assessed by considering its effect on other people; it should be assessed by considering its likely effect on a person subjected to the invasion of privacy.[23]

8.26 Lord Hope in *Campbell v MGN* said that 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*'.[24]

8.27 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.

8.28 The court should also consider the likely harm to a person of 'ordinary sensibilities'. That a particularly sensitive person would be offended or distressed by an invasion of privacy may not be a good indication that the invasion was serious.

Likely harm and actual harm

8.29 The likely effect of the conduct should be distinguished from the actual effect of the conduct. An invasion of privacy may be likely to cause harm, even though in a particular case it does not cause harm, and vice versa. Whether the cause of action should require proof of damage is a related question, discussed separately below.

8.30 The actual effect of the invasion on the plaintiff may give some indication that the invasion of privacy was likely to have that effect, but it would not be conclusive. An invasion of privacy may have been unlikely to have any effect on anyone, or it may have been likely only to have a minor effect on persons of ordinary sensibilities. If the actual plaintiff is highly sensitive and was very much distressed by the invasion, a court might nevertheless consider that a person of ordinary sensibilities would be unlikely to be so distressed, and that therefore the invasion of privacy was not serious.

8.31 It should also be noted that the word 'likely' in Recommendation 8–1 should not be taken to mean 'probable', that is, more likely than not. Rather, 'likely' should mean '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'.[25] Some stakeholders said

---

23 Professor Kit Barker submitted that it was not 'really relevant whether anyone else is offended by the publication of the photograph': K Barker, *Submission 126*.

24 *Campbell v MGN Ltd* [2004] 2 AC 457, [99] (emphasis added).

25 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) (Butler–Sloss P). Cf *Cream Holdings Ltd v Banerjee* (2004) 1 AC 253.

that if this is what the ALRC intends 'likely' to mean, then it should be set out in the Act.[26]

Knowledge and motive of the defendant

8.32 Although the likely effect of the plaintiff's conduct should perhaps be the main focus of the court's inquiry, the motives of the defendant may also suggest an invasion of privacy is serious. An invasion of privacy that was motivated by malice is more likely to be serious. The ALRC recommends that a court consider whether the defendant acted maliciously, when determining whether the invasion of privacy was serious.

8.33 Further, 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 found to be serious, even if a person of ordinary sensibilities might not have been likely to suffer such offence, distress or harm. The court should not be required to 'disregard what the defendant knew or ought to have known about the fortitude of the plaintiff'. These are the words in s 32(4) of the *Civil Liability Act 2002* (NSW), which relates to a confined duty to take care not to cause someone mental harm. The statutory cause of action for serious invasion of privacy should contain a provision similar to s 32(4).

8.34 This provision would also be relevant to the question of the reasonable expectation of the plaintiff in their particular circumstances.

Other factors

8.35 Other relevant factors could also be considered by the court when determining seriousness. For example, the Law Institute of Victoria suggested a court might take into account: 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.[27] It should be made clear in the Act that a court may consider other relevant factors.

A higher threshold?

8.36 Some stakeholders submitted that the threshold should be set higher than 'serious'. The most common alternative threshold suggested by stakeholders was 'highly offensive'.

8.37 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.[28]

---

26 Eg, Law Society of NSW, *Submission 122* ('Given the degree of particularity ascribed to "likely" the BLC recommends that this detail be included in any legislation').

27 Law Institute of Victoria, *Submission 22*.

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–2; Victorian Law Reform Commission, *Surveillance in Public Places*, Report 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.

A 'highly offensive' test was supported by some stakeholders.[29] A 'highly offensive' threshold is also favoured in New Zealand.[30]

8.38 As discussed above, the ALRC considers that the degree of offence caused by an invasion of privacy is one factor to consider when assessing seriousness, but it is not the only factor, nor necessarily the most important. Courts should also consider whether the invasion of privacy was likely to cause distress or harm to dignity, and other matters that make the invasion of privacy serious. In any event, the plaintiff should not be required to prove the invasion of privacy was highly offensive, if it can otherwise be shown to be serious.

Proof of damage not required

Recommendation 8–2 The plaintiff should not be required to prove actual damage to have an action under the new tort.

8.39 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. The tort should be actionable per se.

8.40 If the privacy tort is actionable per se, it will in this respect be similar to other intentional torts that are concerned with the intangible, dignitary interests of the plaintiff—assault, battery and false imprisonment.[31] In a sense, the wrong itself is the harm. Or in other words, the harm is inherent in the wrong.[32]

8.41 The authors of *Markesinis and Deakin's Tort Law* state that 'the function of the interference torts is not to engage in loss-spreading in the same way [as the tort of negligence], but to affirm the fundamental importance of certain constitutional interests, such as personal bodily integrity and freedom of movement, *in their own*

An example of the latter is Gleeson CJ's statement 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': *ABC v Lenah Game Meats* (2001) 208 CLR 199, [42].

29 SBS, *Submission 59*; Australian Bankers' Association, *Submission 27*; Insurance Council of Australia, *Submission 15*. This threshold was supported by some stakeholders who opposed the introduction of the cause of action, perhaps because the threshold is high.

30 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* 3 NZLR 672 [94] (Whata J).

31 On trespass, see *O'Donohue v Wille and Ors* [1999] [1999] NSWSC 661 (6 July 1999); Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) 30; *Letang v Cooper* [1965] 1 QB 232 245. Defamation, while sometimes described as actionable per se, is different in that some damage to reputation is presumed to follow the defamatory publication: *Ratcliffe v Evans* (1892) 2 QB 524, cited in *Ell v Milne (No 8)* [2014] NSWSC 175 (7 March 2014) [69]. There would be no presumption of damage in the new tort. The *Defamation Act 2005* (NSW) s 7(2) provides that the 'publication of defamatory matter of any kind is actionable without proof of special damage'. Note, however, that there is a defence to defamation of triviality.

32 See M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [8.48].

right'.[33] Further, they write, in the torts of trespass to the person and interference with land and with chattels,

> the emphasis is less on the nature of the damage suffered and on whether the defendant's conduct can be characterised as 'fault', as on the nature of the interference with the claimant's rights, in particular on whether it was direct or indirect and on whether, in the context of various defences, it can be characterised as justified or not.[34]

8.42 The ALRC considers that the tort for serious invasion of privacy should have a similar function—it should affirm the fundamental importance of privacy.

8.43 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. That is, harm to the plaintiff is assumed'.[35] 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*.[36]

8.44 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 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.[37] The Public Interest Advocacy Centre 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'.[38] Many stakeholders submitted that the action should not require proof of damage.[39]

8.45 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 many victims of serious invasions of privacy, and significantly undermine the value and purpose of introducing the new tort. If the goal

---

33 Simon F Deakin, Angus Johnston and Basil Markesinis, *Markesinis and Deakin's Tort Law* (Oxford University Press, 2012) 360.

34 Ibid.

35 Warby et al, above n 32, [8.48].

36 Ibid.

37 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.

38 Public Interest Advocacy Centre, *Submission 30*.

39 Office of the Victorian Privacy Commissioner, *Submission 108*; 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*; Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; 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*.

then is to allow plaintiffs to recover damages for emotional distress, the issue is how the law may best achieve this.

8.46 One option would be to require proof of damage but define damage, for the purposes of the action, to include emotional distress. This would be consistent with s 52 of the *Privacy Act*. This provides that the Australian Information Commissioner may make declarations regarding, among other things, redress or compensation for 'loss or damage', which is defined to include:

> (a) injury to the feelings of the complainant or individual; and
>
> (b) humiliation suffered by the complainant or individual.[40]

8.47 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).[41] It is desirable for civil liability under the new tort to be consistent with other civil liability in tort. The ALRC considers that the preferable approach is to make the new tort actionable per se. The threshold of seriousness and the fault element 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 vindication, or, in exceptional circumstances, exemplary damages.

8.48 Some stakeholders supported making the tort actionable per se, arguing that invasions of privacy were 'abhorrent' and that it was important that the cause of action 'establish a clear deterrent'.[42] Others submitted that requiring proof of damage would burden or deter potential litigants.[43]

8.49 The ALRC recommended that plaintiffs should not be required to prove damage in its 2008 privacy report.[44] The recommendation is also consistent with Canadian statutory causes of action.[45]

8.50 It also appears that there is no requirement to prove damage in claims for disclosure of private information under UK law. This is consistent with equitable claims for breach of confidence, where proof of detriment is not required.[46] In practice this issue is not significant as most, if not all, privacy claims in the UK have been

---

40 *Privacy Act 1988* (Cth) s 52(1AB).

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

42 B Arnold, *Submission 28*.

43 Ibid.

44 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–3.

45 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 (British Columbia) s 1(1). See also *Privacy Act*, RSS 1978, c P-24 (Saskatchewan) s 2; *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 2(2); *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador) s 3(1).

46 Dyson Heydon, Mark Leeming and Peter Turner, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2014) 1121.

either for an injunction to prevent an invasive publication or for damages for emotional distress.

8.51 A number of stakeholders submitted that the plaintiff should be required to prove actual damage.[47] 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.[48] For example, the Australian Subscription Television and Radio Association submitted that not requiring proof of damage may 'encourage serial litigants and dubious proceedings'.[49] Free TV Australia said it 'would significantly increase the risk of the cause of action being misused and simply encouraging litigation in circumstances where there is a clear public interest in dissemination of the relevant private information'.[50]

8.52 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'.[51] Telstra suggested that if proof of damage were not required, it would not be an action for 'serious' invasions of privacy: without actual damage, the invasion would not be serious.[52]

8.53 In the ALRC's view, other elements of the cause of action should ensure that frivolous and unmeritorious claims are neither brought nor successful. To have an action under the privacy tort, the plaintiff must prove that he or she had a reasonable expectation of privacy, that the invasion of privacy was intentional or reckless, and that it was serious. The court must also be satisfied that there was no countervailing interest justifying the invasion of privacy. If the plaintiff is able to get over these significant hurdles, it should not be necessary for them to also prove actual damage.

8.54 If a new privacy tort were enacted that required the plaintiff to prove damage, it would be essential that damage include emotional distress.

---

47 ASTRA, *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*.

48 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.

49 ASTRA, *Submission 47*.

50 Free TV, *Submission 109*.

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

52 'If an individual has suffered no damage, an alleged privacy breach should not give rise to a cause of action as a *serious* invasion of privacy': Telstra, *Submission 107* (emphasis in original).

9. Balancing Privacy with Other Interests

Contents

Summary 143
The balancing exercise 144
Other balancing tests 146
No trump card 148
No thumb on the scales 149
Criticisms of balancing 149
Public interest matters 150
Which public interests should be listed? 152
Freedom of expression 152
Freedom of the media 156
Other matters 157
Onus of proof 158
A discrete exercise 161

Summary

9.1 Privacy is an important public interest, but it must be balanced with, and sometimes give way to, other rights and interests.

9.2 Although respecting privacy will promote free expression and the free media necessary for effective democracy, privacy can sometimes conflict with these and other important public interests. Where breaching someone's privacy is justified for an important public interest, privacy must give way.

9.3 In this chapter, the ALRC recommends that, in order for a plaintiff to have a cause of action under a tort for serious invasion of privacy, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest.

9.4 The ALRC also recommends that the Act provide guidance on the meaning of 'public interest', by setting out a list of public interest matters. These include freedom of expression, freedom of the media, public health and safety, and national security.

9.5 The ALRC recommends that competing interests be considered when determining whether the plaintiff has a cause of action. It should be an element of the tort, rather than a defence. A plaintiff should not be able to claim that a wrong has been committed—that their privacy has been seriously invaded—where there are strong public interest grounds justifying the invasion of privacy.

9.6 The defendant will generally be best placed to bring the court's attention to any evidence of countervailing public interests. The ALRC therefore recommends that the

Act should provide that the defendant has the burden to adduce such evidence. The court must then be satisfied that the public interest in privacy outweighs these other public interests. The Act should provide that the plaintiff bears the onus of satisfying the court of this.

The balancing exercise

Recommendation 9–1 The Act should provide that, for the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest. A separate public interest defence would therefore be unnecessary.

9.7 Privacy is an important public interest, but of course there are other important public interests.[1] Sometimes, these other interests should prevail over a person's interest in privacy. There should be a clear process for balancing competing interests, to ensure the new action does not privilege privacy over other important public interests.

9.8 Although there was some disagreement about how and when the balancing exercise should be carried out, stakeholders agreed that a broader public interest may sometimes justify an invasion of privacy, and that this should be recognised in any tort for serious invasion of privacy.[2]

9.9 In *Hosking v Runting*, Gault P and Blanchard J of the New Zealand Court of Appeal discussed how the law should reconcile competing values:

> Few would seriously question the desirability of protecting from publication some information on aspects of private lives, and particularly those of children. Few would question the necessity for dissemination of information albeit involving information about private lives where matters of high public (especially political) importance are involved. Just as a balance appropriate to contemporary values has been struck in the law as it relates to defamation, trade secrets, censorship and suppression powers in the criminal and family fields, so the competing interests must be accommodated in respect of personal and private information.[3]

9.10 The ALRC in 2008 recommended including a balancing exercise as an element of the tort. This was similar to the approach recommended by the New South Wales Law Reform Commission (NSWLRC) in 2009.[4]

---

1 For privacy as a public interest, see Ch 2.

2 The point of disagreement was generally whether it should be an element of the tort, with the plaintiff having the legal onus of proof, or a defence, with the defendant bearing the onus. This is discussed further later in the chapter.

3 *Hosking v Runting* (2005) 1 NZLR 1, [116].

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–2; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 26–29.

9.11 In *Hogan v Hinch*, French CJ said that the 'term "public interest" and its analogues have long informed judicial discretions and evaluative judgments at common law':

> Examples include the enforceability of covenants in restraint of trade, claims for the exclusion of evidence on grounds of public interest immunity, governmental claims for confidentiality at equity, the release from the implied obligation relating to the use of documents obtained in the course of proceedings, and in the application of the law of contempt.[5]

9.12 What is the public interest? In *Reynolds v Times Newspaper*, Bingham CJ said that by 'matters of public interest to the community', he meant:

> matters relating to the public life of the community and those who take part in it, including within the expression 'public life' activities such as the conduct of government and political life, elections … and public administration, but we use the expression more widely than that, to embrace matters such as (for instance) the governance of public bodies, institutions and companies which give rise to a public interest in disclosure, but excluding matters which are personal and private, such that there is no public interest in their disclosure.[6]

9.13 Some of the more notable public interest matters that a court might consider when applying the balancing test recommended by the ALRC are discussed further below. But it may be useful first to consider how this balancing exercise should be carried out.

9.14 The ALRC recommends that Australian courts use a balancing approach similar to that identified by the House of Lords in *Campbell*.[7] In the United Kingdom (UK), 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?[8]

9.15 It is in answering this second question that the balancing exercise is carried out. The correct approach to this balancing exercise, Baroness Hale said in *Campbell*,

> involves looking first at the comparative importance of the actual rights being claimed in the individual case; then at the justifications for interfering with or restricting each of those rights; and applying the proportionality test to each.[9]

---

5 *Hogan v Hinch* (2011) 243 CLR 506, [31] (French CJ).

6 *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127, [19]. This was cited with approval by Lord Phillips in *Flood v Times Newspapers Ltd* [2012] UKSC 12, [33].

7 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) (2002).

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

9 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) (2002), [141]. Gavin Phillipson has written that he had advocated a 'dual exercise in proportionality' or 'parallel analysis' approach, which

9.16 In *Re S,* Lord Steyn said that four propositions emerge clearly from the opinions in the House of Lords in *Campbell*:

> First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each. For convenience I will call this the ultimate balancing test.[10]

9.17 The balancing exercise recommended by the ALRC above is similar to this UK approach. However, although freedom of expression may be the most common interest at stake in actions for serious invasion of privacy, a range of public interests may need to be considered when carrying out this balancing exercise. As recommended below, examples of these many public interests should be set out in the Act.

9.18 Courts also 'balance' public interests for other purposes.[11] The following section briefly outlines three other situations in which courts balance competing public interests.

Other balancing tests

Right to a fair trial

9.19 A person's right to a fair trial is another important public interest that must be balanced against freedom of expression. The classic statement of the relevant principles was made by Jordan CJ in the *Bread Manufacturers* case:

> It is of extreme public interest that no conduct should be permitted which is likely to prevent a litigant in a court of justice from having his case tried free from all matter of prejudice. But the administration of justice, important though it undoubtedly is, is not the only matter in which the public is vitally interested; and if in the course of the ventilation of a question of public concern matter is published which may prejudice a party in the conduct of a law suit, it does not follow that a contempt has been committed. The case may be one in which as between competing matters of public interest the possibility of prejudice to a litigant may be required to yield to other and superior considerations. The discussion of public affairs and denunciation of public abuses, actual or supposed, cannot be required to be suspended merely because the discussion or the denunciation may, as an incidental but not intended by-product,

---

was used in *Campbell*, and under which, 'rather than assigning one right a prior position as a mere exception to the other, the courts would have to consider the matter from the point of view of each Convention right in turn. Such an approach requires courts to assess the weight, in Convention terms, of both rights and ask not only whether the restriction that the applicant sought to lay on the press is greater than necessary to protect his or her legitimate privacy interests, but also, conversely, whether the story goes further, in terms of intrusive detail, than is necessary to fulfil the media's legitimate function': Gavin Phillipson, 'The "Right" of Privacy in England and Strasbourg Compared' in Andrew T Kenyon and Megan Richardson (eds), *New dimensions in privacy law: international and comparative perspectives* (Cambridge University Press, 2006) 184, 214.

10 *Re S* [2005] 1 AC 593, [17].

11 Private interests must also sometimes be balanced by courts. For example, 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.

> cause some likelihood of prejudice to a person who happens at the time to be a litigant.[12]

9.20 Australian civil and criminal courts balance competing public interests in proceedings for contempt of court. The public interest in fair trials is usually weighed against the public interest in freedom of speech. This was made clear by the High Court of Australia in *Hinch v Attorney General (Vic)*, which concerned radio broadcasts about a man charged with various sexual offences, and whether the broadcasts were in contempt of court. There may have been an important public interest in the public being informed about the man's prior conviction and imprisonment, but Toohey J said that these and other considerations 'must in the end be placed in the balance against a precept quite fundamental to our society, that a person charged with an offence is entitled to receive a fair trial':

> The Court is not the arbiter of good taste or literary merit but it must consider the entire content of the broadcasts and ask itself whether their prejudicial effect outweighs the public interest they seek to serve.[13]

9.21 Wilson J said that this balancing exercise 'does not leave editors and publishers at the mercy of discretionary decisions of individual judges':

> [A] decision which is the outcome of the balancing process is not a discretionary judgment. It is the result of an evaluation, consistently with accepted judicial principle, of competing matters of fact.[14]

9.22 Discussing *Hinch*, Spigelman CJ in the NSW Court of Appeal has said that the 'task of balancing conflicting public interests involves the making of a judgment by a process of evaluation':

> It is distinguishable from the making of a finding of fact. It is also distinguishable from the exercise of a discretion, in the sense of a choice between alternative courses of action. Although distinguishable, a process of evaluation will be found, for many jurisprudential purposes, to have a close analogy with fact finding and the exercise of a discretion.[15]

Nuisance

9.23 Tort actions in private nuisance frequently require the courts to balance the interests of the plaintiff with those of the defendant in their respective uses of their

---

12 *Ex parte Bread Manufacturers Ltd; Re Truth & Sportsman Ltd* (1937) 37 SR (NSW) 242, 249–250.

13 *Hinch v Attorney-General (Vic)* (1987) 164 CLR 15, [54] (Toohey J) (Gaudron and Deane JJ also favoured a balancing approach).

14 Ibid [19] (Wilson J). ('The criminal justice system supplies a number of situations where a similar process takes place; for example, the evaluation of negligent conduct causing death to determine whether the negligence is so gross as to justify a verdict of manslaughter, or the consideration of a defence of provocation to a charge of murder. These are not discretionary decisions, any more than the decision whether a publication which would otherwise constitute a contempt of court is saved from punitive consequences because of the circumstances in which it occurred. If the court is left with any reasonable doubt about the answer to that question then of course the prosecution will fail.')

15 *Attorney General (NSW) v X* (2000) 49 NSWLR 653.

land.[16] 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.[17]

9.24 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 perhaps what is reasonable according to the ordinary usages of mankind living in society.[18]

Breach of confidence in the UK

9.25 In the UK, even before the enactment of the *Human Rights Act 1998* (UK), the public interest in preserving confidences would be balanced with freedom of expression. In the *Spycatcher* case, Lord Goff said that,

> although the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure. This limitation may apply... to all types of confidential information. It is this limiting principle which may require a court to carry out a balancing operation, weighing the public interest in maintaining confidence against a countervailing public interest favouring disclosure.[19]

9.26 Lord Griffiths referred to cases in which it was found to be in the public interest that confidential information be disclosed:

> This involves the judge in balancing the public interest in upholding the right to confidence, which is based on the moral principles of loyalty and fair dealing, against some other public interest that will be served by the publication of the confidential material.[20]

No trump card

9.27 It is important to recognise that no one interest should have automatic priority over the privacy interest of the plaintiff. That there may be some important public interest in allowing a serious invasion of privacy should not mean that the plaintiff's interest in privacy may then automatically be ignored. For example, there is an important public interest in a free media, particularly a free media that reports on

---

16 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* 22 FCR 73, 111 (Gummow J).

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

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

19 *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109, 282 (Lord Goff).

20 Ibid 268–269 (Lord Griffiths).

matters of public concern. However, even when reporting on matters of public concern, the media must show some respect for privacy.

9.28 For example, information about a government minister's health will be private, but the minister's interest in privacy may in some cases be outweighed by the public interest in being informed about the health of a person responsible for important public functions. However, even if there is a greater public interest in knowing about the minister's health, this would not mean that a person should be free to use a surveillance device to follow the minister into their doctor's room, or eavesdrop on conversations between the minister and her spouse about the minister's health. There will be limits to how far a person may justifiably invade another person's privacy, even for a genuine public purpose.

9.29 In other words, even important public interests will not always outweigh a plaintiff's privacy interest, because privacy itself is a public interest.

No thumb on the scales

9.30 Is the balance tilted, before the exercise starts? It was submitted by one stakeholder that, considering Australia does not have a right to free speech, then enacting a privacy tort, even with a balancing exercise, will favour privacy interests over freedom of expression. News Corp submitted that the statutory cause of action

> does in fact give 'precedence' to the right to privacy—as it is privacy that has the 'protected' status—by virtue of the statute and the structure of such. Fundamental freedoms and matters of public interest—including freedom of speech and freedom of the press, will therefore be secondary considerations, regardless of the 'balancing' exercise that has been incorporated into the statute. It is therefore difficult to see how elements of a cause of action—for example privacy and freedom of speech—which don't have the same legal status can be truly 'balanced'.[21]

9.31 The tort designed in this Report does not privilege privacy over other public interests. If anything, by requiring the plaintiff to satisfy the court that the public interest in privacy *outweighs* any countervailing public interest, the scales may be tilted slightly in favour of free expression and other public interests. In the presumably rare cases in which a court considers the competing interests are perfectly balanced, this element of the tort will not be satisfied.

Criticisms of balancing

9.32 There are some critics of the process of 'balancing' rights or interests, in the context of privacy claims and in other contexts. Some argued that certain rights and interests should not be qualified. In a paper on the principles of open justice, Spigelman CJ wrote:

> For persons who are advocates of particular interests, or hold a particular intellectual perspective, the terminology of balancing is not always acceptable. The reason is

21 News Corp Australia, *Submission 112*.

> obvious. Balancing necessarily results in occasions when the particular interest or perspective takes second place to some other right or principle.[22]

9.33 Calling something a right is of little value if the right is too readily 'balanced away'. But it is inevitable that rights and values will sometimes clash, so there would seem to be no alternative to qualifying the rights in some respects. Once it is accepted that privacy and freedom of speech are both important rights and will sometimes clash, then it seems inevitable that each right must sometimes be qualified.

9.34 Some also argue that the right balance between competing interests should be found by Parliament, not the courts. However, it is impossible for Parliament to legislate for every situation that may arise. Inevitably, courts will have to make value judgments when adjudicating disputes. In balancing privacy with other public interests, often much will depend on the particular circumstances of the case, so this must be considered by the courts.

9.35 Finally, it should be noted that the balancing test is not an exercise in logic. Rather, it involves evaluating and weighing competing and often incommensurable rights, interests and values.

Public interest matters

Recommendation 9–2 The Act should include the following list of countervailing public interest matters which a court may consider, along with any other relevant public interest matter:

(a) freedom of expression, including political communication and artistic expression;

(b) freedom of the media, particularly to responsibly investigate and report matters of public concern and importance;

(c) the proper administration of government;

(d) open justice;

(e) public health and safety;

(f) national security; and

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

9.36 The ALRC recommends that the Act include a non-exhaustive list of public interest matters that a court may consider when considering whether an invasion of the plaintiff's privacy was justified, because it was in the public interest. 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 (which may in turn reduce

22 James Spigelman, 'The Principle of Open Justice: A Comparative Perspective' (2006) 29 *UNSWLJ* 147, 158.

litigation). This is preferable to including a restrictive definition of 'public interest' in the Act, and to not providing any statutory guidance.

9.37 In *Hogan v Hinch*, French CJ stated that when 'public interest' is used in a statute, 'the term derives its content from "the subject matter and the scope and purpose" of the enactment in which it appears. The court is not free to apply idiosyncratic notions of public interest'.[23]

9.38 In a 2012 report, a UK Joint Committee on Privacy and Injunctions said that the 'worst excesses of the press have stemmed from the fact that the public interest test has been too elastic and has all too often meant what newspaper editors want it to mean'.[24] The Committee emphasised that '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'.[25]

9.39 Including a non-exhaustive list of public interest matters seems more helpful than attempting a definition of public interest, which might necessarily have to be overly general or overly confined and inflexible.[26]

9.40 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 scope of public interest to develop in line with changing community attitudes and developments in technology.

9.41 There is precedent in Australian law and in regulation for providing guidance on the meaning of 'public interest', for example in the public interest exemptions in the *Freedom of Information Act 1982* (Cth).[27]

9.42 A number of stakeholders expressed support for including a non-exhaustive list of factors in the Act.[28] However, the Law Institute of Victoria submitted that the Act should not provide guidance on the meaning of public interest:

> This is a phrase commonly used in legislation and one with which courts are familiar. 'Public interest' is a broad concept that is flexible enough to respond to the facts and

23 *Hogan v Hinch* (2011) 243 CLR 506, [31] (French CJ). This passage follows directly on from the passage quoted earlier in this chapter.

24 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.

25 Ibid. The Committee also recommended that all relevant regulatory bodies 'adopt a common definition of what is meant by the public interest that should be reviewed and updated regularly'.

26 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*.

27 'Factors favouring access to the document in the public interest include whether access to the document would do any of the following: (a) promote the objects of this Act ...; (b) inform debate on a matter of public importance; (c) promote effective oversight of public expenditure; (d) allow a person to access his or her own personal information': *Freedom of Information Act 1982* (Cth) s 11B(3).

28 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*.

> 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.[29]

9.43 Alternatively, broad concepts which go to the meaning of public interest could go in the objects section or the preamble of the Act.

Which public interests should be listed?

9.44 The ALRC recommends that the Act set out public interest matters that are both important and that might sometimes conflict with privacy interests. The list should include: freedom of expression, freedom of the media, the proper administration of government, open justice, public health and safety, national security, and the prevention and detection of crime and fraud. Freedom of expression and freedom of the media are perhaps the interests that will most commonly conflict with a privacy interest, so these are discussed further below.

9.45 Many of these matters are also referred to in the list of exceptions to the right to respect for private and family life in art 8 of the *European Convention on Human Rights*. Article 8 provides that there should be 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.[30]

9.46 The following section discusses two public interests that may sometimes conflict with privacy.

Freedom of expression

9.47 The public interests that will perhaps most commonly conflict with privacy are freedom of expression and freedom of the media.[31]

9.48 The vital importance of free speech and free expression is of course now rarely seriously disputed in democratic countries, and the subject of a vast legal and philosophical literature. Article 19 of the *International Covenant on Civil and Political Rights* provides, in part:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[32]

---

29 Law Institute of Victoria, *Submission 22*.

30 *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).

31 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.

32 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) Art 19(2).

9.49 Those who oppose the introduction of a new privacy tort commonly appeal to the fundamental right to freedom of expression, and argue that the tort will impede free speech and a free media. The ALRC is particularly concerned that the tort recommended in this Report does not have that effect. The public interest in freedom of speech and freedom of the press should be expressly recognised in an Act providing for a new privacy tort. This may be particularly important, given Australia has not enshrined a right to free speech in its law in the way other democracies have, such as the United States in the First Amendment to its *Constitution*, and the United Kingdom in its *Human Rights Act 1988* (UK).

9.50 That it will sometimes be justified to limit free speech to protect people's privacy is implicit in a tort for invasion of privacy. But the public interest in free speech should not easily be outweighed by privacy interests. Lord Hoffmann has said that

> a freedom which is restricted to what judges think to be responsible or in the public interest is not freedom. Freedom means the right to publish things which government and judges, however well motivated, think should not be published. It means the right to say things which 'right-thinking people' regard as dangerous or irresponsible.[33]

9.51 The public interest balancing exercise recommended in this chapter is designed to ensure that privacy interests give way to free speech, when this is in the public interest.

9.52 Nevertheless, freedom of speech is not absolute, and must be balanced against certain other public interests, including the public interest in privacy.[34] Chief Justice Mason of the High Court of Australia said in *Australian Capital Television v Commonwealth*:

> In most jurisdictions in which there is a guarantee of freedom of communication, speech or expression, it has been recognized that the freedom is but one element, though an essential element, in the constitution of 'an ordered society' or a 'society organized under and controlled by law'. Hence, the concept of freedom of communication is not an absolute. The guarantee does not postulate that the freedom must always and necessarily prevail over competing interests of the public.[35]

9.53 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. In *Campbell,* Baroness Hale 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

---

33 *R (Mrs) v Central Independent Television Plc* [1994] Fam 192, 202–203.

34 Lord Hoffmann said that many impressive and emphatic statements about free speech in the law reports are 'often followed by a paragraph which begins with the word "nevertheless". The judge then goes on to explain that there are other interests which have to be balanced against press freedom.' Lord Hoffmann suggests that these exceptions are sometimes made too hastily. But he also said freedom of speech is 'subject only to clearly defined exceptions laid down by common law or statute'.

35 *Australian Capital Television v Commonwealth* (1992) 177 CLR 106, [45] (Mason J).

> 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.[36]

9.54 Professor Eric Barendt has said that there are dangers in discriminating between more and less worthy speech, but 'lines and distinctions have to be drawn, unless the privacy right is to be altogether eviscerated'.[37]

9.55 The speech that is most privileged in Australian law is political communication. It is, to use Baroness Hale's words, 'top of the list' of speech deserving protection, because it is crucial to any democracy. The Australian High Court has found that freedom of political communication is implied in the *Australian Constitution*. In *Lange v ABC*, the High Court said:

> Freedom of communication on matters of government and politics is an indispensable incident of that system of representative government which the Constitution creates by directing that the members of the House of Representatives and the Senate shall be 'directly chosen by the people' of the Commonwealth and the States, respectively. At federation, representative government was understood to mean a system of government where the people in free elections elected their representatives to the legislative chamber which occupies the most powerful position in the political system ... Communications concerning political or government matters between the electors and the elected representatives, between the electors and the candidates for election and between the electors themselves were central to the system of representative government, as it was understood at federation.[38]

9.56 It is clear that political communication should be given considerable weight in the balancing exercise recommended by the ALRC. It may be that only rarely will the public interest in privacy outweigh the public interest in free and open political discourse. The ALRC recommends that the Act make clear that the public interest in political communication is to be given considerable weight in the balancing exercise, by including the words 'political communication' after 'freedom of expression' in the list of public interest matters. In any case, courts would no doubt give particular weight to political communication. Chief Justice French of the High Court has said that freedom of expression

> can inform the construction and characterisation, for constitutional purposes, of Commonwealth statutes. It can also inform the construction of statutes generally and the construction of delegated legislation made in the purported exercise of statutory powers. As a consequence of its effect upon statutory construction, it may affect the scope of discretionary powers which involve the imposition of restrictions upon freedom of speech and expression.[39]

---

36 *Campbell v MGN Ltd* [2004] 2 AC 457, [148].

37 'It makes sense to say that free political speech is of prime importance and that, therefore, the media are entitled to report that a minister is having an extra-marital affair and so trump her privacy right. It makes much less sense to make this claim, when the claimant is a footballer or film star': Eric Barendt, 'Privacy and Freedom of Speech' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006) 11, 20.

38 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 559–60.

39 *Attorney-General (South Australia) v Corporation of the City of Adelaide* (2013) 249 CLR 1, [44].

9.57 What is political communication? In *Theophanous v The Herald and Weekly Times*, Mason CJ, Toohey and Gaudron JJ said that political discussion includes:

> discussion of the conduct, policies or fitness for office of government, political parties, public bodies, public officers and those seeking public office. The concept also includes discussion of the political views and public conduct of persons who are engaged in activities that have become the subject of political debate, eg, trade union leaders, Aboriginal political leaders, political and economic commentators. Indeed, in our view, the concept is not exhausted by political publications and addresses which are calculated to influence choices.[40]

9.58 The judges then quoted Barendt, who wrote that

> 'political speech' refers to all speech relevant to the development of public opinion on the whole range of issues which an intelligent citizen should think about.[41]

9.59 It should be noted, however, that even freedom of political communication is not absolute in Australia. Legislation will only be invalid on account of the freedom 'where it so burdens the freedom that it may be taken to affect the system of government for which the *Constitution* provides and which depends for its existence upon the freedom'.[42]

9.60 Politicians and others in public office are of course entitled to some degree of privacy. Not all invasions of the privacy of public figures can be characterised and justified as political speech. Much will depend on whether a particular communication can be properly characterised as political communication in the first place.

9.61 Other types of expression are of course also very important, and should sometimes not be restricted, even where the expression invades someone's privacy. Stakeholders including the ABC, the Arts Law Centre and the National Association for the Visual Arts submitted that 'artistic expression' be specifically mentioned in the list of public interest matters.[43] In discussing the relative merits of different types of speech, Baroness Hale also referred to the importance of intellectual, educational and artistic expression.[44]

---

40 *Theophanous v The Herald and Weekly Times* (1994) 182 CLR 104, 124.

41 Ibid, [14].

42 'In *Lange*, it was also said that the freedom of political communication is limited to what is necessary for the effective operation of the system of representative and responsible government provided for by the Constitution. … The Court was there explaining that the freedom is not absolute … In *APLA Ltd v Legal Services Commissioner* (NSW), Gleeson CJ and Heydon J observed that the freedom was not a general freedom of communication of the kind protected by the United States Constitution. The point sought to be made in *Lange* and in *APLA* was that legislation which restricts the freedom is not invalid on that account alone': *Unions NSW v State of New South Wales* (2013) 88 ALJR 227, [18]–[19].

43 Arts Law Centre of Australia, *Submission 113*; ABC, *Submission 93*; National Association for the Visual Arts Ltd, *Submission 78*.

44 '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': *Campbell v MGN Ltd* [2004] 2 AC 457, [148].

Freedom of the media

9.62 The ALRC recommends that the list of public interests should include the freedom of the media to investigate, and inform and comment on matters of public concern and importance. This is intended to highlight the vital public interest in responsible journalism on matters of genuine public interest. In his book on freedom of speech, Barendt wrote:

> The media provide readers, listeners, and viewers with information and that range of ideas and opinion which enables them to participate actively in a political democracy. Put shortly, the media perform a vital role as the 'public watchdog'. As the 'eyes and ears of the general public' they investigate and report the abuse of power. So the argument from democracy, overall the most persuasive rationale for the free speech principle, justifies the coverage of mass media communications.[45]

9.63 However, the public interest in a free press will not justify all invasions of privacy. In fact, invasions of privacy by the media may sometimes be harder to justify than a similar invasion by someone else, because of the harm that might come from the greater publicity. Barendt has written that '[m]edia gossip is quite different in its impact from village gossip':

> I do not suggest that the argument for a free press and media is not a strong one, or that it is not entitled to great weight in privacy as in other civil and criminal proceedings. But press freedom is parasitic to some extent on the underlying free speech rights and interests of readers and listeners, and the role which the press and other media play in informing them. It is not the same as a free speech argument, and that should be borne in mind when we consider how much weight should be attached to the freedom when it conflicts with the right to privacy which certainly is a fundamental human right.[46]

9.64 It is sometimes argued that, because freedom of speech and the media is so fundamental to democracy, anything that limits the media is necessarily harmful to democracy. However, modern day media organisations have a very wide spectrum of activities and interests. On the same website on which may be found news and analysis of important political and social matters, may often be found photos of celebrities at the beach. Publishing such photos may be justified on some grounds, but hardly in the name of democracy. Courts when balancing a person's privacy interests with the public interest should naturally give relatively little weight to a newspaper's interest in publishing entertaining gossip, but considerable weight to the importance of newspapers publishing material on matters of genuine public concern.[47]

---

45 Eric Barendt, *Freedom of Speech* (Oxford University Press, 2nd ed, 2007) 417–8.

46 Eric Barendt, 'Privacy and Freedom of Speech', in Andrew T Kenyon and Megan Richardson, *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006) 23.

47 Des Butler expressed a related concern about 'embellished' reporting. He submitted that in 'neither the case of a statutory cause of action nor uniform surveillance laws should free rein be given to sloppy or embellished reporting under the cover of the public interest': D Butler, *Submission 74*.

Other matters

9.65 Other matters that should be included in the non-exhaustive list of public interest matters are: the proper administration of government; open justice; public health and safety; national security; and the prevention and detection of crime and fraud.

9.66 These matters attracted relatively little comment in submissions to the Discussion Paper. Some stakeholders said that the 'proper administration of government' is too broad'.[48] The UNSW Cyberspace Law and Policy Community said that proper administration should 'privilege key personal rights and interests such as privacy over mere administrative convenience'.[49] The National Archives suggested instead: 'the proper administration of government including administrative responsibilities pursuant to any laws'.[50]

9.67 The ABC and the Law Institute of Victoria questioned whether 'national security' should be included, considering that invasions of privacy necessary for national security would be protected by the separate defence for 'lawful activity'.[51]

9.68 Guardian News and Media Limited and Guardian Australia also expressed concern about 'national security' and 'economic wellbeing of the country':

> While these are clearly important public interests, it is important to ensure that their recognition in this context does not permit avoidance by governments of other laws which require appropriate processes, such as the obtaining of valid search or surveillance warrants by police, to protect privacy and guard the important protections provided by due process. [52]

9.69 In the Discussion Paper, the ALRC included in the proposed list of public interest matters, 'the economic wellbeing of the country'. Although no doubt this will sometimes be a public interest, it is perhaps too general, and therefore unhelpful, to include in the list.[53]

9.70 The Australian Privacy Foundation expressed concern about the 'excessive generality, scope and difficulty in definition of matters particularly around administration of government, the economic wellbeing of the country, and the defence of "legal authority". These are not appropriate or appropriately narrowly limited, and so could seriously undermine the effectiveness of the proposed cause of action'.[54]

---

48 Australian Privacy Foundation, *Submission 110*; National Archives, *Submission 100*; UNSW Cyberspace Law and Policy Community, *Submission 98*.

49 UNSW Cyberspace Law and Policy Community, *Submission 98*.

50 National Archives, *Submission 100*.

51 Law Institute of Victoria, *Submission 96*; ABC, *Submission 93*.

52 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

53 See, eg, Australian Privacy Foundation, *Submission 110*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Human Rights Commission, *Submission 75*. Concerning 'the economic wellbeing of the country', the Australian Human Rights Commission said that depending on how it is interpreted, it 'could be used to dismiss privacy for legitimate private information, commercial or others, or for potentially unjustified and perceived interest for the public that may not amount to legitimate public interest'.

54 Australian Privacy Foundation, *Submission 110*.

9.71 Telstra submitted, with respect to 'national security' and 'the prevention and detection of crime and fraud', that they 'should be extended to include all law enforcement activities, for example investigation, prevention, detection and prosecution of crime and fraud'.[55] Telstra also said that 'the protection of public revenue could also be considered'.[56]

Private interests

9.72 In the Discussion Paper, the ALRC proposed that a court should be satisfied that 'the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest'.[57] However, the ALRC now recommends that the focus be on balancing the *public interest in privacy* with any countervailing public interests. Privacy is not merely a private interest, but also an important public interest.[58] The private interests of the parties, such as in privacy or free expression, will generally reflect the broader public interests at stake. But the focus of this element of the tort should be on the public interest—the question of whether this *type* of invasion of privacy may be justified on public interest grounds.

Onus of proof

Recommendation 9–3 The Act should provide that the defendant has the burden of adducing evidence that suggests there is a countervailing public interest for the court to consider. The Act should also provide that the plaintiff has the legal onus to satisfy the court that the public interest in privacy outweighs any countervailing public interest that is raised in the proceedings.

9.73 Should the plaintiff be required to prove that the public interest in privacy outweighs any countervailing public interest? Or should the defendant be required to prove that the public interest outweighs the privacy interest? This was one of the more difficult questions raised in this Inquiry.

9.74 The ALRC has concluded that, if a court considers that the privacy interests and public interests at stake in a particular case are evenly weighted, then the plaintiff should not have a cause of action. The plaintiff should be required to satisfy the court that the public interest in privacy outweighs any countervailing public interests. 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

55 Telstra, *Submission 107*.
56 Ibid.
57 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) Proposal 8–1.
58 See Ch 2.

> competing public interest. Quite simply, privacy only needs protection if it is not outweighed, in the circumstances, by such a competing interest.[59]

9.75 The alternative approach of making public interest a defence carries a risk that the cause of action would be used to stifle or 'chill' activities that are socially desirable, particularly the operations of the media.

9.76 Some stakeholders said that the plaintiff should have the onus of proof. 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.[60]

9.77 To make this decision, a court must have some evidence before it. Although the ultimate legal burden will remain with the plaintiff, the ALRC recommends that the Act provide that the defendant has the burden of adducing any evidence of public interest.[61] The defendant should usually be in a better position to provide evidence that the invasion of privacy was in the public interest.[62] A newspaper, for example, will generally be better placed to bring evidence of the public interest in free speech than a person whose privacy the newspaper has invaded. The Law Institute of Victoria submitted that evidence will be required, for example, 'about why the privacy breach occurred and why the defendant acted in the way they did—evidence that can only be provided by the defendant'.[63]

9.78 In some cases, the public interest will be obvious or raised in the plaintiff's pleadings. In other cases, where no evidence is raised of countervailing public interests, the court may not need to balance competing interests, and this element of the tort will

---

59 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 28. This was also the approach recommended by the ALRC in 2008: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [17.157].

60 Telstra, *Submission 45*. See also, SBS, *Submission 59*; ASTRA, *Submission 47*.

61 This is the evidential burden—ie, 'the obligation to show, if called upon to do so, that there is sufficient evidence to raise an issue as to the existence or non-existence of a fact in issue, due regard being had to the standard of proof demanded of the party under such obligation': Dyson Heydon, *Cross on Evidence* (Lexis Nexis Butterworths, 9th ed, 2012) [7105] (citations omitted). The legal burden of proof, on the other hand, is 'the obligation of a party to meet the requirement of a rule of law that a fact in issue be proved (or disproved) either by a preponderance of the evidence or beyond reasonable doubt, as the case may be': Ibid [7010]. On the distinction between the legal onus of proof and the evidentiary or strategic onus of proof, see also Bob Williams, 'Burdens and Standards in Civil Litigation' (2003) 25 *Sydney Law Review* 165.

62 Law Institute of Victoria, *Submission 96*. Dr Normann Witzleb: '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': 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. See also Australian Privacy Foundation, *Submission 39*; Public Interest Advocacy Centre, *Submission 30*; D Butler, *Submission 10*.

63 Law Institute of Victoria, *Submission 96*. However, in making this point, the LIV also said that 'the defendant should not be required to put on evidence until the cause of action has been established; that is, as a defence to a serious invasion of privacy'. The ALRC considers that the evidentiary and legal burden can be separated, so that the defendant has the onus to adduce evidence, but the plaintiff the onus to prove on the balance of probabilities that the privacy interest outweighs any public interest.

be satisfied. The plaintiff will not have to separately plead and prove the non-existence of public interests that have not been raised.

9.79 Although some stakeholders submitted that a balancing exercise should be carried out when determining actionability,[64] as the ALRC has recommended, others submitted that there should instead be a public interest defence, and that the defendant should bear the burden of proof.[65] Associate 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).[66]

9.80 The Victorian Law Reform Commission (VLRC) argued 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'.[67]

9.81 New Zealand has a defence of 'legitimate public concern' to invasions of privacy.[68] The Court of Appeal of New Zealand stated, in *Hosking v Runting*, that it was 'more conceptually sound' for the absence of legitimate public interest to be treated as a defence, rather than as an element of the tort itself, 'particularly given the

---

64 Arts Law Centre of Australia, *Submission 113*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; National Association for the Visual Arts Ltd, *Submission 78*; Google, *Submission 54*; ASTRA, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*.

65 Women's Legal Services NSW, *Submission 115*; Office of the Victorian Privacy Commissioner, *Submission 108*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Sex Party, *Submission 92*; Office of the Australian Information Commissioner, *Submission 66*; 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*; B Arnold, *Submission 28*; Australian Bankers' Association, *Submission 27*; Law Institute of Victoria, *Submission 22*; Pirate Party of Australia, *Submission 18*; D Butler, *Submission 10*; T Gardner, *Submission 3*. (Stakeholders generally did not distinguish between a legal and evidentiary burden).

66 M Paterson, *Submission 60*.

67 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) recs 27, 28.

68 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* 3 NZLR 672, [96].

parallels with breach of confidence claims'.[69] There are also public interest defences to privacy torts in Canada.[70]

9.82 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'.[71]

9.83 However, the ALRC considers that it is preferable to consider the public interest when determining actionability at the outset, 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.

A discrete exercise

9.84 The ALRC has recommended a discrete public interest balancing exercise. Another option is to have public interest matters considered when determining whether the plaintiff had a reasonable expectation of privacy.[72]

9.85 Public interest matters will sometimes be relevant to the question of whether the plaintiff had a reasonable expectation of privacy. For example, if private information is published about a politician, the fact that the information is about a politician may be relevant both to the question of whether the politician had a reasonable expectation of privacy, and to whether the publication of the information is in the public interest.

9.86 At other times, it may be artificial to consider public interest matters when determining whether the plaintiff had a reasonable expectation of privacy.

9.87 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.

---

69 *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."'

70 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: see, eg *Privacy Act*, RSBC 1996, c 373 s 2(3)(a).

71 Maurice Blackburn Lawyers, Submission No 45 to DPM&C Issues Paper, 2011 (citations omitted).

72 That the plaintiff must have a reasonable expectation of privacy is another element of the cause of action: Rec 8–1.

> 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.[73]

9.88 However, 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.

73 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 19.

10. Forums, Limitations and Other Matters

Contents

Summary 163
Forums 164
Federal courts 164
State and territory courts 165
Cost management in courts 166
Tribunals 167
The role of government regulatory bodies 168
Alternative dispute resolution processes 168
No requirement to pursue ADR 169
No bar on judicial proceedings after ADR 170
Cause of action limited to natural persons 171
Privacy action remedies a personal interest 171
Non-survival of the cause of action 172
Privacy action protects personal interests 172
Actions by affected parties 173
International consistency 176
Representative and class actions 176
Limitation periods 177
Extending limitation period 180
Young plaintiffs 181
First publication rule 182

Summary

10.1 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.

10.2 The ALRC recommends that federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy.

10.3 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 (OAIC). Failing to pursue such alternative dispute resolution processes should not bar a plaintiff from bringing an action under the new tort. However, the ALRC recommends that the 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 (ADR) process.

10.4 The chapter then discusses who should have standing to sue for a serious invasion of privacy. The ALRC recommends that the plaintiff must be a natural person, rather than a company or other organisation. The ALRC also recommends that the new tort should not survive in favour of a plaintiff's estate or against a defendant's estate. These recommendations reflect the fact that privacy is a matter of personal sensibility.

10.5 The ALRC recommends a limitation period of either one year from the date on which the plaintiff became aware of the invasion of privacy or three years from the date on which the invasion of privacy occurred, whichever occurs first. In exceptional circumstances, the court may extend this limitation period, but the period should expire no later than six years from the date on which the invasion occurred. The ALRC also recommends that consideration be given to extending the limitation period where the plaintiff was under 18 years of age when the invasion of privacy occurred.

10.6 The ALRC recommends that consideration should be given to enacting a 'first publication rule', also known as a 'single publication rule'. This would limit the circumstances in which a person may bring an action in relation to the publication of private information, when that same private information had already been published in the past.

Forums

Recommendation 10–1 Federal, state and territory courts should have jurisdiction to hear an action for serious invasion of privacy under the Act. Consideration should also be given to giving jurisdiction to appropriate state and territory tribunals.

10.7 The ALRC recommends that jurisdiction to hear actions for serious invasions of privacy under the Act should be conferred upon federal, state and territory courts. This position was widely supported by stakeholders. The ALRC considers it inappropriate to restrict the particular state and territory courts that may hear these actions.

10.8 In reaching this recommendation, the ALRC has taken into account a range of factors, including: the importance of access to justice; 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.

10.9 The plaintiff's particular choice of court will likely depend on the jurisdictional limits of the various courts and the nature of the remedy sought by the plaintiff. The jurisdictions of the various courts are considered briefly below.

Federal courts

10.10 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 Commonwealth Acts such as the *Bankruptcy Act 1966* (Cth), the

Migration Act 1958 (Cth), the Australian Consumer Law,[1] the *Corporations Act 2001* (Cth), the *Telecommunications Act 1997* (Cth) and the *Privacy Act 1988* (Cth) (*Privacy Act*). As the ALRC recommends in Chapter 4, the new tort should be located in a Commonwealth Act, and this statute could vest power to hear actions in the FCA and the FCCA.

10.11 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 and burden for plaintiffs.

10.12 Both the FCA and the FCCA have, in addition to jurisdiction granted to them by legislation, 'associated jurisdiction'[2] and 'accrued jurisdiction'[3] for matters, not otherwise within these courts' respective jurisdictions, that are related to matters which are within their respective jurisdictions. For example, while no statute 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 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.[4]

10.13 However, the ALRC considers that the FCA and the FCCA should not have exclusive jurisdiction[5] to hear actions under the 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

10.14 State and territory courts include supreme courts, district or county courts, and local or magistrates courts. The Act, as a Commonwealth law, could vest federal jurisdiction in state and territory courts to hear the new cause of action.[6]

---

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

2 *Federal Court of Australia Act 1976* (Cth) s 32; *Federal Circuit Court of Australia Act 1999* (Cth) s 18.

3 *Stack v Coastal Securities (No 9)* (1983) 154 CLR 261.

4 See, eg, *Dale v Veda Advantage Information Services and Solution Limited* [2009] FCA 305 (1 April 2009).

5 The power to grant exclusive jurisdiction to federal courts is provided to the Commonwealth under s 77(ii) of the *Australian Constitution*. For an example of exclusive jurisdiction of the Federal Court, see *Competition and Consumer Act 2010* (Cth) s 86.

6 This vesting of jurisdiction is possible under ss 71 and 77(iii) of the *Australian 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.

10.15 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.[7]

10.16 District and county courts (and the ACT Magistrates Court) generally have similar powers to supreme courts, including powers to grant injunctions and equitable remedies.[8] 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.[9]

10.17 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;[10] and the Magistrates Court of South Australia has powers limited to certain procedural functions, adjourning proceedings, certain statutory matters, and 'minor civil actions'.[11] 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.[12] Local and magistrates courts typically do not have the power to grant an injunction.

10.18 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

10.19 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,[13] 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.[14] While these mechanisms will not remove the costs for all litigants, they do temper the costs associated with court

---

7 See, eg, *Supreme Court Act 1970* (NSW) s 23; *Constitution Act 1975* (Vic) s 85(1).

8 *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.

9 *County Court Act 1958* (Vic) ss 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.

10 *Local Court Act 2007* (NSW) s 33.

11 *Magistrates Court Act 1991* (SA) ss 8, 10, 15.

12 See, eg, *Magistrates Court (Civil Proceedings) Act 2004* (WA) s 6.

13 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.

14 *Civil Procedure Regulation 2012* No 393 (NSW) reg 11.

proceedings in some cases. The ALRC also suggests that courts be empowered to make a range of costs orders.[15]

Tribunals

10.20 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 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).[16] These tribunals have a range of powers including, in some cases the power to grant injunctions.[17]

10.21 The appropriateness of these tribunals for dealing with privacy matters has been previously noted. 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.[18]

10.22 There was general agreement among stakeholders that low-cost forums for hearing actions for serious invasions of privacy would be beneficial. Some stakeholders were in favour of state and territory tribunals being able to hear such cases. For example, the Redfern Legal Centre submitted that

> several states and territories have created tribunals that are able to hear civil matters. The advantage of these tribunals is that they provide a relatively efficient and cost-effective way to resolve disputes and thereby allow a wider section of the community to access justice. We believe, for example, that the [*Privacy and Personal Information Protection Act 1998* (NSW)] is much more effective in protecting the privacy rights of individuals in NSW because it includes a right of review in the NSW Civil and Administrative Tribunal (NCAT).[19]

10.23 Other stakeholders were less supportive of state and territory tribunals being empowered to hear actions for serious invasions of privacy. The Law Institute of Victoria, for example, submitted that they

> would be wary of establishing jurisdiction for (VCAT) to hear claims about serious invasions of privacy, because there is likely to be complex legal argument as the tort

---

15 See Ch 12.

16 *South Australian Civil and Administrative Tribunal Act 2013* (SA). This Act provides for the establishment of the South Australian Civil and Administrative Tribunal (SACAT). However, at the time of writing, the SACAT had not begun operation.

17 *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).

18 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.226].

19 Redfern Legal Centre, *Submission 94*.

> develops. Courts, and specifically judges, are best placed to hear and determine these types of disputes. Further, the rules of evidence do not apply in VCAT matters.[20]

10.24 The Domestic Violence Legal Service and the North Australian Aboriginal Justice Agency were similarly cautious about empowering tribunals to hear actions under the Act, noting that

> There may be some advantages in terms of cost and less formality for disadvantaged litigants in approaching a Tribunal rather than a Court, however, currently in the Northern Territory the Administrative Appeals Tribunal sits infrequently and so is not as readily accessible as the courts.[21]

10.25 The powers and nature of state and territory tribunals differ significantly, and any conferral of power on these tribunals would need to take these differences into account. State and territory governments would then be in a position to enact legislation, if necessary, to confer jurisdiction on appropriate tribunals.

The role of government regulatory bodies

10.26 The OAIC proposed that it should be able to hear complaints about serious invasions of privacy.[22] The OAIC's proposal received support from several stakeholders.[23]

10.27 The OAIC's proposal is discussed in greater detail in Chapter 16. The ALRC recommends that consideration be given to extending the powers of the Commissioner to allow investigations of complaints about serious invasions of privacy in general, in addition to the Commissioner's existing power to hear complaints about breaches of the *Privacy Act.*

Alternative dispute resolution processes

10.28 An individual should be able to bring an action for serious invasion of privacy under the Act regardless of whether or not the individual has already taken steps to resolve the complaint through an ADR process. However, a court may take into account any reasonable steps taken by either party to resolve a dispute without litigation, and the outcome of any ADR process. Stakeholders were generally supportive of this position.

10.29 Complaints about serious invasions of privacy may be made to statutory bodies. These include, in particular, to the OAIC, the Australian Communications and Media Authority (the ACMA), state and territory privacy commissioners and ombudsmen. The ALRC also recommends that the Australian Government give consideration to empowering the Privacy Commissioner to investigate complaints about invasions of

---

20 Law Institute of Victoria, *Submission 96*.
21 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*.
22 Office of the Australian Information Commissioner, *Submission 90*; Office of the Australian Information Commissioner, *Submission 66*.
23 Australian Privacy Foundation, *Submission 110*; Australian Communications Consumer Action Network, *Submission 106*; G Greenleaf, *Submission 76*.

privacy beyond those invasions currently falling within the *Privacy Act*.[24] Various industry bodies also provide ADR processes.

10.30 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. However, the speed and availability of ADR processes may vary, depending on the allocation of public resources.

10.31 If a statutory cause of action for serious invasion of privacy were 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.

10.32 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. However, the ALRC suggests that courts should have a wide discretion, when determining any amount of damages, to take into account whether parties took reasonable steps the to avoid litigation.[25]

No requirement to pursue ADR

10.33 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,[26] and a number supported only voluntary ADR.[27]

10.34 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

---

24 See Ch 16.

25 See Ch 12 and in particular Rec 12–2.

26 Optus, *Submission 41*; Australian Bankers' Association, *Submission 27*; Law Institute of Victoria, *Submission 22*; Office of the Information Commissioner, Queensland, *Submission 20*.

27 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*.

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.

10.35 Moreover, barring plaintiffs from initiating ADR without first pursuing non-judicial proceedings would present a significant restriction on 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.

10.36 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.[28]

10.37 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).[29] 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 conciliations, and those investigative powers would not be triggered in such circumstances.[30]

No bar on judicial proceedings after ADR

10.38 The ALRC does not recommend that a complainant who has received a determination from an ADR process should be barred from initiating judicial proceedings about the same matter.

10.39 It is undesirable for individuals to 'double-dip' by receiving compensation through both court and ADR processes. However, a bar on individuals commencing court proceedings after ADR would present a serious limitation on access to justice and discourage the use of ADR processes.

---

28 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*.

29 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.

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

10.40 Furthermore, the risk of a complainant double-dipping is likely to 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.

Cause of action limited to natural persons

Recommendation 10–2 The new tort should only be actionable by natural persons.

10.41 The ALRC recommends that the statutory cause of action for serious invasion of privacy be limited to natural persons.[31] This means that corporations, government agencies or other organisations[32] would not have standing to sue for invasions of privacy. This recommendation was unanimously supported by previous law reform inquiries.[33]

Privacy action remedies a personal interest

10.42 An action in privacy is designed to remedy a personal, dignitary interest. It would be incongruous, therefore, to assign this interest to a corporation or other body. In *Australian Broadcasting Corporation v Lenah Game Meats,* Gummow and Hayne JJ held that any common law tort of unjustified invasion 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'.[34]

10.43 In support of this argument, Guardian News and Media Limited and Guardian Australia argued that

> Privacy is fundamentally an interest limited to natural persons. The parallel right for corporations and other non-natural entities is confidential information which is already sufficiently protected.[35]

10.44 Similarly, PIAC argued that 'it would be incongruous to assign this interest to a corporation or other body'.[36]

---

31 Several stakeholders supported this recommendation: T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Telstra, *Submission 107*; Public Interest Advocacy Centre, *Submission 105*; ASTRA, *Submission 99*; Australian Sex Party, *Submission 92*; Google, *Submission 91*; Australian Bankers' Association, *Submission 84*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; Barristers' Animal Welfare Panel and Voiceless, *Submission 64*.

32 Including elected bodies: *Ballina Shire Council v Ringland* (1994) 33 NSWLR 680.

33 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 32; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–3(a); NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWLRC Draft Bill, cl 74(1).

34 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [126].

35 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

36 Public Interest Advocacy Centre, *Submission 105*.

10.45 Actions in defamation, which are analogous to privacy actions, are also, generally speaking, limited to living, natural persons.[37] Similarly, only individuals may bring a complaint under the *Privacy Act*.[38]

Non-survival of the cause of action

Recommendation 10–3 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.

10.46 The ALRC recommends that an action for serious invasion of privacy should not survive the death of a plaintiff.

10.47 This recommendation 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. Furthermore, actions cannot subsist against the estate of a deceased person, whether or not proceedings had commenced before the death of the defendant. This recommendation has a similar effect to the provisions of the Uniform Defamation Laws.[39]

10.48 Several stakeholders supported this recommendation.[40] All previous law reform inquiries into a new privacy action recommended that a cause of action be restricted to living persons.[41]

Privacy action protects personal interests

10.49 The new tort is intended to remedy a wrong committed against a person's dignitary interests. The mischief to be remedied by a privacy action is the mental harm and hurt to feelings suffered by a living person.[42] The ALRC therefore considers that only the individual who has suffered loss or damage should be able to sue for relief, and that the action should be limited to living persons.[43] 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).[44]

---

37 See, eg, *Defamation Act 2005* (SA) 2005 s 9. Some small businesses (which employ fewer than 10 employees), and not for profit organisations have standing under the Act to sue for defamation.

38 *Privacy Act 1988* (Cth) s 36(1).

39 See, eg, *Defamation Act 2005* (NSW) 2005 s 10. The Tasmanian Act does not include this provision.

40 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Bankers' Association, *Submission 84*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

41 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008); Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 32; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) Draft Bill, cl 79.

42 Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy*, (2004) [29].

43 Several stakeholder supported this position: Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*; Insurance Council of Australia, *Submission 15*.

44 Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [11.53], [28.38]. This rule has been abrogated in relation to many claims.

10.50 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.[45]

10.51 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.[46] 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.[47] However, breach of confidence actions protect quasi-proprietary 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.

10.52 Even where actions currently 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. It is generally not possible to recover damages for pain, suffering and the mental harms that would be the most likely result of a serious invasion of privacy.[48]

10.53 Some stakeholders submitted that the action could survive in some specific circumstances. For example, PIAC argued that the action should survive the death of a plaintiff where 'important systemic issues are involved'.[49] PIAC suggested that the value of privacy as a matter of public interest is akin to the public value in eliminating discrimination and should therefore survive the death of a complainant for the good of all society.

10.54 Some areas of anti-discrimination law recognise the survival of certain interests in certain circumstances. For instance, s 93(1) of the *Anti-Discrimination Act 1977* (NSW) provides that a discrimination complaint survives the death of the complainant. It could be argued, however, that any damages payable to an estate for an invasion of the privacy of a deceased person, would amount to a windfall to that person's estate to the benefit of beneficiaries who may not have been harmed in any way by an invasion of privacy.

Actions by affected parties

10.55 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—

---

45 Public Interest Advocacy Centre, *Submission 30*.
46 See, eg, *Defamation Act 2005* (SA) s 10.
47 Law Institute of Victoria, *Submission 22*.
48 *Law Reform (Miscellaneous Provisions) Act 1946* (NSW) s 2.
49 Public Interest Advocacy Centre, *Submission 30*. See, also, I Turnbull, *Submission 81*.

for example, a surviving family member who also suffered distress caused by the invasion of the deceased person's privacy while the latter was alive.[50]

10.56 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.

10.57 Dr Ian Turnbull argued that the action should survive for the benefit of

> immediate relatives or individuals within relevant organisations, that can establish prima facie loss or damage to themselves, as a result of the disclosure of the information.[51]

10.58 However, in such cases it would be possible for family members or other parties to pursue their own actions for serious invasion of privacy where they meet the tests for actionability in their own right.[52] 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,[53] or in circumstances where a deceased's medical record is published to disclose a condition affecting surviving relatives. 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.[54]

10.59 PIAC and Dr Normann Witzleb argued that it may be appropriate to allow family members to pursue actions, but limit the remedies available. For instance, PIAC submitted that

> It is appropriate, however, to limit the remedies available to the estate. The Ireland Law Reform Commission proposed that the cause of action is extinguished only in relation to 'the remedy of damages or an account of profits so that injunctive relief, delivery up and other relief remain available.[55]

10.60 PIAC argued that an action should survive the death of a person in particularly egregious cases, such as where systemic issues are involved. In such cases, PIAC argued that the harm incurred extends beyond that experienced by the relevant individual or their family, and is therefore a societal harm:

> As an invasion of privacy is a societal (as well as an individual) wrong, the continuation of a cause of action for invasion of privacy after a person's death may assist in achieving the societal objects of the proposed legislation, regardless of whether or not it results in a personal remedy.[56]

10.61 Several stakeholders argued that privacy actions should survive the death of a plaintiff where the wrong involved an online invasion of privacy.[57] Due to the nature of

---

50 I Turnbull, *Submission 81*.
51 Ibid.
52 SBS, *Submission 59*; NSW Young Lawyers, *Submission 58*; ASTRA, *Submission 47*.
53 NSW Young Lawyers, *Submission 58*; Public Interest Advocacy Centre, *Submission 30*.
54 *Krahe v TCN Channel Nine Pty Ltd* (1986) 4 NSWLR 536.
55 Public Interest Advocacy Centre, *Submission 105*.
56 Ibid.
57 N Witzleb, *Submission 116*; UNSW Cyberspace Law and Policy Community, *Submission 98*.

the internet, online invasions of privacy may be ongoing, compounding the harm caused by the initial invasion of privacy.

10.62 Witzleb argued that the

> The digital afterlife of a person can provide a fertile ground for disputes, including how a deceased person's private information should be handled. The new privacy tort should provide redress in these and other cases involving the privacy interests of a deceased person.[58]

10.63 To illustrate this problem, PIAC gave the example of the defacement of tribute pages on social media sites which are established in dedication of deceased persons.[59]

10.64 This example was also used by UNSW Cyberspace Law and Police Community when highlighting two circumstances surrounding death and serious invasions of privacy:

> (1) the potential for breaches of privacy to be directly linked to a person's cause of death through a variety of means, and (2) an increasing trend of harassment and defacement of on-line and off-line memorials which cause great distress and damage to families and loved ones. The outrage caused by the public defacement of online memorials in the Trinity Bates murder highlight the privacy tort as an additional or alternative avenue of legal redress. The suicide of Tyler Clementi in the US after secretly filmed footage of him kissing another man was posted online further emphasises the scope and impact of privacy threats in the digital era. For these reasons we consider it important that in line with earlier observations (ALRC Issues Paper 43 para [110]) that serious invasion of privacy action persist to the plaintiff's estate.[60]

10.65 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 Aboriginal or Torres Strait Islander, given the specific cultural beliefs of those communities associated with mourning and death.[61] In these cases, it was suggested, a family or other affected party should be able to bring the claim on behalf of the deceased person.

10.66 Similarly, the Domestic Violence Legal Service and the North Australian Aboriginal Justice Agency argued that

> Family members of the deceased should be able to bring an action, for example, children of a deceased parent who is the subject of sexually explicit material posted online.[62]

10.67 The ALRC recommends a general principle of non-survival of the action, considering that in circumstances where a family member of an affected party experience an invasion of privacy in their own right, this will give rise to a separate action.

---

58 N Witzleb, *Submission 116*.
59 Public Interest Advocacy Centre, *Submission 30*.
60 UNSW Cyberspace Law and Policy Community, *Submission 98*.
61 Arts Law Centre of Australia, *Submission 43*; Law Institute of Victoria, *Submission 22*.
62 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*.

10.68 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'.[63]

10.69 The Australian Privacy Foundation argued that a court may consider the financial circumstances of a deceased defendant when awarding remedies against their estate.[64] 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.

International consistency

10.70 Limiting the action for statutory invasion of privacy to living persons would, generally speaking, bring Australian law into line with international privacy law.[65] PIAC noted, however, the exception of French law which allows family members to bring civil privacy actions on behalf of a deceased relative.[66] An example is the 2007 case of *Hachette Filipacchi Associés (Paris-Match) v France*.[67] German and Italian law also allow some protection for the privacy interests of deceased persons.[68]

Representative and class actions

10.71 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.[69]

10.72 The ALRC makes no recommendations on the availability of representative or class actions, as the ALRC considers existing court 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. Rules also exist relating to representative and class actions, as well as the appointment of litigation guardians in circumstances where an individual does not have the capacity to commence or defend legal proceedings.[70] This would include the availability of litigation guardians for minors.

10.73 The *Australian Securities and Investments Commission Act 2001* (Cth) provides for a court to make orders that apply to a class of 'affected individuals', even where

---

63 Law Institute of Victoria, *Submission 22*.
64 Australian Privacy Foundation, *Submission 39*.
65 See, eg, *Privacy Act*, RSBC 1996, c 373 (British Columbia) s 5.
66 Public Interest Advocacy Centre, *Submission 30*.
67 *Hachette Filipacchi Associés (Paris-Match) v France* (2009) 49 EHRR 515.
68 N Witzleb, *Submission 116*.
69 Office of the Australian Information Commissioner, *Submission 66*; B Arnold, *Submission 28*; Pirate Party of Australia, *Submission 18*.
70 Bernard Cairns, *Australian Civil Procedure* (Thomson Reuters (Professional) Australia, 8th ed, 2009) [9.580].

those individuals are not subject to the proceedings.[71] 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.

10.74 The Law Society of NSW Young Lawyers' Committee on Communication, Entertainment and Technology recommended vesting power in the OAIC to bring actions on behalf of a deceased person.[72] This approach would require significant reform 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.

10.75 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.[73] 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 new tort. At the same time as this Inquiry the ALRC is 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 recommendations will have relevance to any new statutory cause of action for serious invasion of privacy.[74]

Limitation periods

Recommendation 10–4 A person should not be able to bring an action under the new tort after the earlier of:

(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.

Recommendation 10–5 In exceptional circumstances, the court may extend this limitation period, but the period should expire no later than six years from the date on which the invasion occurred.

10.76 This recommendation aims to balance the interests of both parties to a proceeding, providing adequate time for a plaintiff to appreciate and manage the

71 *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.

72 NSW Young Lawyers, *Submission 58*.

73 Office of the Public Advocate (Queensland), *Submission 12*.

74 Australian Law Reform Commission, *Equality, Capacity and Disability in Commonwealth Laws*, Discussion Paper 81 (2014).

emotional and financial repercussions of a serious invasion of privacy, while also providing certainty for defendants.

10.77 In most cases, a person whose privacy has been invaded will become aware of the invasion of privacy soon after it occurs. Intrusions upon physical seclusion will often be known immediately. If private information is published in popular media, again the subject of the information will usually know of its publication quite soon. If they wish to bring an action, they should generally do so within one year from the date on which they became aware of the invasion of privacy.

10.78 A reasonable but confined limitation period will protect defendants from claims relating to incidents that occurred years before and where witnesses may have difficulty recalling events. It would be burdensome on defendants if 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.

10.79 Professor Peter Handford outlines three policy rationales for limitation periods: to protect defendants from claims relating to incidents which occurred years before about which witnesses may have difficulty recalling events or finding records; to encourage quick resolution of litigation; and to provide finality for defendants.[75]

10.80 The recommendation is consistent with the one year limitation period prescribed for actions in defamation.[76] Consistency with the position in defamation law may avoid the risk that plaintiffs will bring multiple actions at different times for overlapping harm. Defamation actions are based on damage to a person's reputation, a harm which is complete on publication. In some cases, the same publication may be an invasion of privacy because it discloses private information.

10.81 In contrast to actions in defamation, actions in personal injury, which generally have a longer limitation period of three years,[77] are based on injury to the individual which may take longer to eventuate.

10.82 This recommendation is also consistent with the limitation periods in the *Privacy Act* with respect to when the OAIC can hear complaints.[78] 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.[79] The OAIC then has discretion as to whether or not to investigate a complaint of privacy interference made

---

75 Peter Handford, *Limitation of Actions: The Laws of Australia* (Thomson Reuters (Professional) Australia, 3rd ed, 2012) [5.10.120].

76 *Limitation Act 1969* (NSW) s 14B; *Limitation Act 1985* (ACT) s 21B(1); *Limitation Act 1981* (NT) s 12(2)(b); *Limitation of Actions Act 1974* (Qld) s 10AA; *Limitation of Actions 1936* (SA) s 37(1); *Defamation Act 2005* (Tas) s 20A(1); *Limitation of Actions Act 1958* (Vic) s 51(1AAA); *Limitation Act 2005* (WA) s 15.

77 See, eg, *Limitations of Actions Act 1958* (Vic) s 5(1AA); *Limitation Act 1969* (NSW) s 18A(2).

78 *Privacy Act 1988* (Cth) s 41(1)(c).

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

after this date. The OAIC supports the application of a similar limitation period to a statutory cause of action for serious invasion of privacy.[80]

10.83 Several stakeholders supported a one year limitation period, although some said a court should be able to extend the limitation period beyond three years.[81] The New South Wales Law Reform Commission proposed a one year limitation period.[82] Several stakeholders supported a one year limitation period, in line with defamation law.[83] ASTRA argued that a one year limitation period would provide certainty to defendants and encourage the timely and proper administration of justice.[84] Furthermore, ASTRA argued that a short limitation period would prevent plaintiffs from delaying bringing proceedings in order to gain a windfall in damages caused by the accumulation of hurt or distress.

10.84 In some circumstances, a person may not know for some time that their privacy has been breached.[85] Where a plaintiff does not know of an invasion of privacy for some time, the ALRC recommends that they have three years from the date on which the invasion of privacy occurred to bring an action.

10.85 A number of stakeholders said that a one year limitation period was too short,[86] and that the period should run from the date when the plaintiff first becomes aware of the action.[87] The Victorian Law Reform Commission proposed a three year limitation period, consistent with actions for personal injury.[88] Several stakeholders proposed a limitation period of three years from the date when the plaintiff becomes aware of the invasion, expiring no more than six years from the date on which the invasion occurs.[89] SBS said the limitation period should start from the 'initial publication or disclosure'.[90]

10.86 The limitation periods for the new tort should not start when damage accrued to the plaintiff. Commencing the limitation period from the date when a plaintiff experiences damage or harm as a result of the invasion of privacy, would require a plaintiff to demonstrate damage, thus conflicting with the ALRC's recommendation that the new privacy tort be actionable per se.

10.87 By way of comparison, defamation actions run from the date of publication.[91] Actions in personal injury commence from the date of discoverability. In NSW,

---

80 Ibid.

81 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; Australian Bankers' Association, *Submission 84*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

82 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [9.1].

83 Telstra, *Submission 107*; ASTRA, *Submission 99*; ABC, *Submission 93*; SBS, *Submission 59*.

84 ASTRA, *Submission 99*.

85 UNSW Cyberspace Law and Policy Community, *Submission 98*.

86 N Witzleb, *Submission 29*.

87 Ibid.

88 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.248] and Rec 33.

89 Law Institute of Victoria, *Submission 96*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*; N Witzleb, *Submission 29*.

90 SBS, *Submission 59*.

91 See, eg, *Limitation Act 1969* (NSW) s 14.

'discoverability' is taken to be from when the plaintiff 'ought to have known' that the 'injury or death concerned has occurred'.[92]

10.88 Some stakeholders argued for much longer limitation periods. One pointed to the six year limitation period for those seeking remedial relief for unlawful interception under s 107B of the *Telecommunications (Interception and Access) Act 1979* (Cth). Some stakeholders suggested there should be no limitation period at all. However, the ALRC considers that it is important that there be a limitation period, and that concerns about unfairly denying a person the opportunity to bring an action may be met by allowing the court to extend the limitation period in exceptional circumstances.

Extending limitation period

10.89 The ALRC recommends that, in exceptional circumstances, the court should be able to extend the limitation period to six years, from the date when the serious invasion of privacy occurred.

10.90 Several stakeholders also argued that individuals may be too distressed to turn their minds to bringing legal action to redress the invasion of their privacy.[93] The Law Institute of Victoria (LIV) said that 'it takes time for people to realise that they have a legal right that has been breached, especially where they have been seriously affected by the breach itself'.[94] It was also submitted that victims of family violence may 'find it hard to gain the necessary strength and resources to bring an action within a short period.[95] These are some examples of the sort of exceptional circumstances in which a court may extend the limitation period.

10.91 Some stakeholders submitted that a court should only be able to extend the limitation period to three years.[96] Others said the court should be able to extend it further.[97] Some suggested that applications for time extensions were expensive and vigorously fought, and that it would therefore be better simply to make the standard limitation period longer.[98]

10.92 Limitation periods may be extended or postponed at the discretion of a court in a number of circumstances.[99] The *Limitation Acts* in all Australian jurisdictions allow for the grant of an extension where the plaintiff is a person living with a disability or where there is fraud or mistake. In NSW, most actions are subject to an ultimate bar of 30 years, with some exceptions for actions in wrongful death and personal injury.[100]

---

92 Ibid s 50D.
93 Women's Legal Services NSW, *Submission 115*; Public Interest Advocacy Centre, *Submission 105*; Law Institute of Victoria, *Submission 22*.
94 Law Institute of Victoria, *Submission 96*.
95 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*.
96 ABC, *Submission 93*.
97 Women's Legal Services NSW, *Submission 115*; Public Interest Advocacy Centre, *Submission 105*; N Witzleb, *Submission 29*.
98 See, eg, Law Institute of Victoria, *Submission 96*.
99 Handford, above n 75, [5.10.2150].
100 *Limitation Act 1969* (NSW) s 51(2).

10.93 Defamation law 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'.[101]

10.94 There are many circumstances where courts are asked to consider extensions where it is 'just and reasonable' to both parties to a proceeding.[102] Section 23A(3) of the *Limitation Act 1969* (NSW) includes a non-exhaustive list of matters that a court may reconsider when extending a limitation period for actions in personal injury. The matters include:

> (a) the length of and reasons for the delay on the part of the plaintiff;
>
> (b) the extent to which, having regard to the delay, there is or is likely to be prejudice to the defendant;
>
> (c) the extent, if any, to which the defendant had taken steps to make available to the plaintiff means of ascertaining facts which were or might be relevant to the cause of action of the plaintiff against the defendant;
>
> (d) the duration of any disability of the plaintiff arising on or after the date of the accrual of the cause of action;
>
> (e) the extent to which the plaintiff acted promptly and reasonably once he knew that the act or omission of the defendant, to which the injury of the plaintiff was attributable, might be capable at that time of giving rise to an action for damages;
>
> (f) the steps, if any, taken by the plaintiff to obtain medical, legal or other expert advice and the nature of any such advice he may have received.

Young plaintiffs

Recommendation 10–6 Consideration should be given to extending the limitation period where the plaintiff was under 18 years of age when the invasion of privacy occurred.

10.95 This recommendation aims to assist plaintiffs who claim their privacy was invaded when they were under 18 years of age. Minors cannot generally be expected to make the difficult personal and financial decision to commence legal proceedings.[103] Limitation periods should therefore start from the date of their 18th birthday.

---

101 Ibid s 56A; *Defamation Act 2005* (SA) 2005 s 56A.

102 *Limitation of Actions Act 1958* (Vic) s 27K(2)(b).

103 This recommendation is informed by the discussion in Ch 2 on the often acute effects of invasions of privacy on children and young people, particularly in the context of privacy invasions which occur online or through the use of mobile phones.

10.96 There are analogous provisions for the application of limitation periods on actions affecting minors in civil liability legislation in several Australian jurisdictions.[104]

First publication rule

> **Recommendation 10–7** Consideration should be given to enacting a 'first publication rule', also known as a 'single publication rule'. This would limit the circumstances in which a person may bring an action in relation to the publication of private information, when that same private information had already been published in the past.

10.97 Once private information has been wrongly published once, the subsequent publication of that information by the same person should not generally give rise to a new cause of action. The enactment of a 'first publication rule', also known as a 'single publication rule', would in effect focus the action on the first publication of the private information. It would also reduce the number of actions brought for serious invasions of privacy.

10.98 This rule may be particularly important for organisations that publish archives of material. If a newspaper invaded someone's privacy in 2014, the person generally should not be able to bring an action for invasion of privacy in 2020, merely because the material remains published in an archive on the newspaper's website.

10.99 Several stakeholders recommended the introduction of a single publication rule, but did not suggest a particular model or formulation of the principle.[105] Were such a rule to be introduced, it would be desirable for it to be consistent across defamation law and the new tort.

10.100 The 'first publication rule' diverges from the longstanding principle in defamation law that each publication of defamatory material gives rise to a separate cause of action, which is subject to its own limitation period (the 'multiple publication rule').[106] This multiple publication rule has been said to raise

> significant problems due to the possibility of 'continuous' or 'perpetual' publication in online archives. While internet material remains online and available to be accessed, whether directly or in archives, the limitation period is effectively open-ended, with a fresh limitation period starting to run each and every time defamatory material is accessed online.[107]

---

104 For example, in some Australian jurisdictions, an action for personal injury where an injury or death occasioned to a minor was caused by a parent or guardian is 'discoverable' by the victim when the victim turns 25 years of age: *Limitation of Actions Act 1958* (Vic) s 27I; *Limitation Act 1969* (NSW) s 50E.

105 Media and Communications Committee of the Law Council of Australia, *Submission 124*; ABC, *Submission 93*.

106 See, eg, *Defamation Act 2005* (NSW) 2005 s 4. See, also, *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575.

107 Jennifer Ireland, 'Defamation 2.0: Facebook and Twitter' (2012) 56 *Media & Arts Law Review* 53, 66.

10.101 The UK legislature adopted a single publication rule in s 8 of the *Defamation Act 2013* (UK), which may provide a useful model for such a provision for the new tort, as well as for defamation law in Australia. The UK Act provides for a 'single publication rule' to prevent an action being brought in relation to republication of the same material by the same publisher after one year from the date of first publication. The cause of action is therefore treated for limitation purposes as accruing from the date of first publication. The limitation period may be set aside under the discretion allowed to the court.

10.102 The provision does not apply where the subsequent publication is 'materially different' from the first publication.[108] A court may consider, among other things, 'the level of prominence that a statement is given' and 'the extent of the subsequent publication', when determining whether a publication is materially different from the first publication.[109] The Explanatory Notes offer an example:

> where a story has first appeared relatively obscurely in a section of a website where several clicks need to be gone through to access it, but has subsequently been promoted to a position where it can be directly accessed from the home page of the site, thereby increasing considerably the number of hits it receives.[110]

10.103 If a first publication rule were enacted in Australia, care should be taken in its application to minors. If the privacy of a minor is invaded, the limitation period should start when the minor turns 18, not when the material is first published.

108 *Defamation Act 2013* (UK) s 8(4).
109 Ibid s 8(5)(a)–(b).
110 Explanatory Notes, Defamation Bill 2013 UK s 8.

11. Defences and Exemptions

Contents

Summary 185
Lawful authority 186
Required by law 188
Authorised by law 189
Consequential amendments to existing legislation 191
Incidental to the exercise of a lawful right of defence of persons or property 191
Necessity 193
Consent 195
Express and implied consent 198
Onus of proof 199
Revocation and withdrawal of consent 200
Absolute privilege 202
Publication of public documents 204
Fair report of proceedings of public concern 206
Safe harbour scheme for internet intermediaries 207
Conditions 210
Exemption or defence for children and young persons 211
Defences unsuited to a privacy action 213
Other defamation defences 213
Contributory negligence 216
Other defences and exemptions 217

Summary

11.1 The ALRC recommends a number of defences that would limit a plaintiff's right to succeed under the new tort. The defences reflect the need to protect, and in some cases privilege, important countervailing interests above a plaintiff's expectation of privacy. Defendants will bear the onus of proving that their conduct is subject to a defence or exemption. The recommended defences are:

- lawful authority to protect defendants from liability under the new privacy tort where their conduct was required or authorised by law;
- conduct incidental to the exercise of a lawful right of defence of persons or property, where that conduct was proportionate, necessary and reasonable, and where the defendant reasonably believed that the conduct was necessary to protect persons or property;

- necessity where a defendant acts in a reasonable belief that they were preventing an imminent and greater harm; and
- consent including express and implied consent.

11.2 The ALRC also recommends a number of defences which are the same as, or analogous to, defamation defences: absolute privilege; publication of public documents; and fair and accurate reporting of public proceedings.

11.3 This chapter discusses several matters that will not give rise to a defence because defences would be superfluous in view of the elements of the tort or actionability. Because the balancing test for actionability already protects public interest, a defence of public interest is unnecessary. There is also no need for a defence that the material was already in the public domain, because this issue will be considered when deciding at the outset whether the plaintiff has a reasonable expectation of privacy at the relevant time.

11.4 Contributory negligence will not be a defence to an intentional or reckless invasion of privacy.

11.5 The ALRC considers that a number of defences to defamation are inappropriate for an action for intentional or reckless invasion of privacy. These include the defences of qualified privilege, truth, innocent dissemination and comment.

11.6 This chapter includes a recommendation for a safe harbour scheme for internet intermediaries to exempt internet hosts and platform providers from liability provided they meet certain conditions.

Lawful authority

Recommendation 11–1 The Act should provide for a defence that the defendant's conduct was required or authorised by law.

11.7 The defence of lawful authority protects a defendant from liability for serious invasions of privacy where the conduct was required or authorised by law.[1] This defence will be especially important for government authorities that are required to maintain law, order, safety and governance in a manner consistent with their statutory powers. The exercise of their responsibilities will often, necessarily, encroach on private rights.

1 A number of stakeholders supported this defence: N Witzleb, *Submission 116*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Telstra, *Submission 107*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; 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*; B Arnold, *Submission 28*.

11.8 Statutory bodies whose roles and responsibilities are prescribed by state, territory and federal legislation, include government agencies and departments, security and intelligence organisations and law enforcement agencies. This defence is necessary to protect organisations from civil liability for performing legitimate activities pursuant to statutory authority, such as law enforcement agencies intercepting telephone conversations under warrant.

11.9 This defence is consistent with the principle that any licence for public bodies or officials to pursue conduct that may infringe the fundamental rights or interests of an individual must be clearly and unambiguously authorised 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]

11.10 The defence of statutory authority to intentional torts provides that public bodies and officials do not have a licence to commit acts, which would otherwise be unlawful or tortious—unless authorised by statute.[3] This defence may protect individuals and agencies from civil suits where a defendant's conduct was performed under statutory authority to prevent and detect crime; in exercise of powers of arrest; and in the provision of public utilities and services.[4]

11.11 Areas of the criminal law also provide defences for lawful authority. For example, s 10.5 of the *Commonwealth Criminal Code 1995* provides that a person 'is not criminally responsible for an offence if the conduct constituting the offence is justified or excused by or under law'.[5]

11.12 Previous law reform reports recommended a defence of lawful authority.[6] The New South Wales Law Reform Commission (NSWLRC) noted that the defence of statutory authority is necessary to enable 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.[7] Activities that may otherwise amount to an invasion of privacy have been shown to be very effective in the apprehension of offenders.[8]

---

2 *Coco v R* (1994) 179 CLR 427, [8]–[9] (Mason CJ, Brennan, Toohey, Gaudron and McHugh JJ).
3 Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [6.49].
4 Ibid.
5 The Criminal Code is set out as the schedule to the *Criminal Code Act 1995* (Cth).
6 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.194]; NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008).
7 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) 43.
8 For example, 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).

11.13 The AFP provided examples of statutory obligations authorising the procurement of an individual's private information.[9] For example, the *Australian Federal Police Act 1979* (Cth) 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.[10]

11.14 The AFP submitted that its activities are already subject to a range of existing internal and independent 'accountability frameworks'.[11] However, the ALRC considers it is appropriate for the statutory cause of action to provide civil redress for individuals whose privacy has been invaded, in the event that an agency acts outside any lawful authority.[12]

11.15 The AFP raised the concern that any unmeritorious litigation could divert resources away from important law enforcement and security operations.[13] However, the ALRC considers that the thresholds built into the statutory cause of action and the defence of lawful authority will prevent unmeritorious claims proceeding to trial.

11.16 Similarly, the AFP was concerned that 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 or investigation.

11.17 The ALRC considers, however, that there are strong protections in the court system to mitigate this risk. These protections include closed court proceedings and other protective measures provided by federal, state and territory legislation.[14]

Required by law

11.18 In the Discussion Paper, the ALRC proposed 'a defence of lawful authority'.[15] Several stakeholders submitted that any such defence should be extended to a defence

---

9 Australian Federal Police, *Submission 67*.

10 Ibid.

11 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 member of the Administrative Appeals Tribunal to consider whether an individual's privacy would be interfered with by interception through the use of a warrant.

12 Or a person for whose conduct it is vicariously liable: Australian Federal Police Act 1979 (Cth) s 64B; *Law Reform (Vicarious Liability) Act 1983* (NSW) Pt 4. See, further, Balkin and Davis, above n 3, 772.

13 Australian Federal Police, *Submission 67*.

14 See, eg, *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

15 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) Proposal 10–1.

for actions 'required by law',[16] in order to capture the activities of statutory agencies and their officers who are legally mandated to undertake certain activities. For example, the National Archives argued that including 'required by law' would broaden the defence to include the use and release of records pursuant to the *Archives Act 1983* (Cth).

11.19 The term 'authority' includes circumstances where someone is empowered or has the discretion to pursue certain lawful conduct.[17] The term 'requires' indicates an imperative to take some specific action, without the exercise of discretion, and is narrower. Arguably, conduct which is 'required by law' will also fall within the term 'authorised by law'. However it is important to ensure that government bodies and other entities and individuals are not sued for carrying out activities they are legally obliged to undertake. Therefore the ALRC recommends that the defence should include the phrase 'required by law'.

Authorised by law

11.20 The term 'lawful' is intended to give effect to federal, state and territory legislative and non-legislative instruments. The defence should include authority given under: Commonwealth, state and territory acts and delegated legislation; an order of a court or tribunal; and documents that are given the force of law by an act, such as industrial awards.[18]

11.21 Under the defence, any act or course of conduct committed under statutory authority will be protected from liability. That authority, as canvassed by the High Court in *Coco v R*, must be 'express'.[19]

11.22 'Lawful' should also extend to documents which have the 'force of the law'. A document may have the 'force of law' if it is an offence to breach its provisions, or if it is possible for a penalty lawfully to be imposed if its provisions are breached.[20]

11.23 Dr Normann Witzleb argued that the defence of lawful authority is unnecessary: where an authorised person exercises their statutory authority, they are necessarily authorised to commit that action.[21] However, the ALRC considers a clear defence will provide certainty to parties.

11.24 The AFP also suggested that law enforcement agencies should have a total exemption from liability, because liability may inhibit the legitimate activities of law enforcement and intelligences agencies, causing agencies to change established and efficient modes of operation.[22] In the digital era, there is increasing community concern

16 Office of the Victorian Privacy Commissioner, *Submission 108*; National Archives, *Submission 100*; Australian Bankers' Association, *Submission 84*.
17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [16.72].
18 Ibid [13.44].
19 *Coco v R* (1994) 179 CLR 427.
20 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) [16.22].
21 N Witzleb, *Submission 116*; N Witzleb, *Submission 29*.
22 Australian Federal Police, *Submission 67*.

and debate over the extent of surveillance and data collection carried out by public agencies. The ALRC considers that it is not appropriate that public agencies should be exempt or immune from liability for serious invasions of privacy. However, a defence for conduct required or authorised by law will give appropriate protection.[23]

11.25 The Human Rights Committee of the Law Society of NSW was concerned that agencies could rely on the defence of lawful authority for the gathering of metadata. The Committee noted that the defence would mean that the new cause of action would not protect individuals from the collection of metadata or surveillance by security or other government agencies authorised by legislation—'which would appear to be the majority of such data collection and surveillance'.[24] Its concern was that legislation authorising the collection of metadata breaches Australia's human rights obligations. Some of the legislation the Committee refered to is the subject of other current inquiries.[25]

11.26 Some stakeholders argued that a qualification that the conduct was just, reasonable[26] and/or necessary[27] should attach to the defence to curb excesses of power. The UNSW Cyberspace Law and Policy Community argued that the defence is too 'broad', suggesting it should be qualified by 'elements of transparency, necessity, justification, effectiveness and proportionality'.[28] However, the ALRC considers that the only relevant question should be whether or not the conduct was authorised by law. In some cases, the legislation authorising the conduct will already build in qualifying matters such as that the conduct was reasonable or necessary, for it to be considered lawful.

11.27 It is also implicit in the defence that the conduct must have been for the purposes of the lawful authority and not for an ulterior purpose. This is illustrated by *Donnelly v Amalgamated Television Services Pty Ltd,* where Hodgson CJ in Eq said:

> If police, in exercising powers under a search warrant or of arrest, were to enter into private property and thereby obtain documents containing valuable confidential information... I believe they could in a proper case be restrained, at the suit of the owner of the documents, from later using that information to their own advantage, or to the disadvantage of the owner, or passing the information on to other persons for them to use in that way.[29]

---

23 N Witzleb, *Submission 116*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Telstra, *Submission 107*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; 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*; B Arnold, *Submission 28*.

24 Law Society of NSW, *Submission 122*.

25 See Ch 1.

26 Australian Bankers' Association, *Submission 84*.

27 N Witzleb, *Submission 29*.

28 UNSW Cyberspace Law and Policy Community, *Submission 98*.

29 *Donnelly v Amalgamated Television Services Pty Ltd* (1998) 45 NSWLR 570, (Hodgson CJ in Eq). This was quoted by Gleeson CJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 230 [53].

11.28 The Business Law Committee of the Law Society of NSW referred to the concern of insolvency practitioners who are often met with objections on 'privacy' grounds when carrying out their investigations.[30] Investigations or requests for, or disclosures of, information would generally be authorised by contractual rights underpinning the process or the defence of lawful authority. The latter would operate where legislation provided for the relevant process, such as the *Corporations Act 2001* (Cth), in the case of corporate insolvency and administration, or the *Bankruptcy Act 1966* (Cth) for personal insolvency, or pursuant to an order of a court—for example, for the appointment of a trustee, receiver or liquidator.

Consequential amendments to existing legislation

11.29 The enabling acts of all statutory bodies should not need to be amended to protect their actions from liability when done as required or authorised by those acts. In some circumstances, however, it may be appropriate to amend specific legislation so that existing exemptions from civil liability extend to the new tort.

11.30 For example, s 57(1) of the *Archives Act 1983* (Cth) provides:

> Where, in the ordinary course of the administration of this Act, access is given to a record as being a record required by this Part to be made available for public access:
>
> (a) no action for defamation, breach of confidence or infringement of copyright lies, by reason of the authorizing or giving of the access, against the Commonwealth or any person concerned in the authorizing or giving of the access.

11.31 Although it may be unnecessary, given the defence of lawful authority, this provision could be amended by adding a reference to actions for serious invasion of privacy. While the defence that the conduct was authorised or required by law should be sufficient protection to authorised activities, consequential amendments to s 57 of the *Archives Act* may provide greater certainty and consistency.

Incidental to the exercise of a lawful right of defence of persons or property

Recommendation 11–2 The 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.

11.32 The defence will arise in several circumstances: self-defence; defence of another person; and defence of property.[31]

---

30 Law Society of NSW, *Submission 122*.

31 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]; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) rec 74–4.

11.33 The requirement that the conduct be proportionate, necessary and reasonable is an important qualification. In tort law, the question of whether a defendant's conduct was proportionate and reasonable is a question of fact.[32] The qualification that conduct be 'reasonable, proportionate and necessary' will provide a court with the opportunity to balance competing interests.[33] This qualification to the defence reflects concepts of proportionality and reasonableness found generally in tort law and in human rights jurisprudence.[34] As noted in Chapters 2 and 9, privacy is an interest which must be viewed in the context of competing interests and assessments of proportionality. The balancing process in this defence is consistent with other elements of the cause of action, specifically the reasonable expectation of privacy and the public interest test.[35]

11.34 The recommended defence to an invasion of privacy should arise only where the defendant has reasonable grounds for believing that the conduct was necessary, which is analogous to the position at common law in tort.[36] The ALRC considers that the objectivity of this condition is desirable in view of the wide range of conduct that may be involved in an invasion of privacy.

11.35 A defendant acting in an emergency would also have the defence of necessity in some of the circumstances that would come within this defence.

11.36 The defence will also protect individuals from liability where their conduct protects a third party from harm. The conduct is more likely to be considered necessary and reasonable where that third party is under the individual's care or responsibility, such as a member of their family, or where that third party is incapable of exercising self-defence, but the defence would not be limited to such circumstances. At common law, the defence extends to protection of an individual's household, employer, family members and even, in some circumstances, strangers.[37]

11.37 The defence would also protect individuals from liability where their conduct was in defence of property, although different weight is given to the defence of property compared with the defence of persons.[38] This is analogous to the defence for intentional torts where a defendant's conduct in response to a threat or harm to their property is reasonable.[39]

---

32 Balkin and Davis, above n 3, [6.15].

33 Law Institute of Victoria, *Submission 22*.

34 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: UN Human Rights Committee, General Comment No 29, UN Doc CCPR/C/21/Rev1/Add11 (2001).

35 The ABC submitted that the qualification of proportionality is 'appropriate' and consistent with media guidelines including their Editorial Policies and Code of Practice: ABC, *Submission 46*.

36 *Ashley v Chief Constable of Sussex Police* [2008] 2 WLR 975. In that case, it was held that a reasonable, though mistaken belief, in a threat of danger is sufficient to ground self-defence. Cf *Civil Liability Act 2002* (NSW) s 52.

37 Balkin and Davis, above n 3, [6.17]. The defence of another person in criminal law has been codified in some Australian jurisdictions: *Criminal Code Act 1995* (Cth) cl 10.4; *Civil Liability Act 2002* (NSW) s 52.

38 Balkin and Davis, above n 3, [6.18].

39 This defence in criminal law is codified in some Australian jurisdictions, for example: *Criminal Code Act 1899* (Qld) s 274. In tort law, civil liability legislation also applies to defences of property: see, eg, the *Civil Liability Act 2002* (NSW) s 52.

11.38 The defence that conduct was incidental to the defence of persons or property operates in the statutory causes of action for 'violation of privacy' in a number of Canadian provinces. The precise provisions vary:

- British Columbia,[40] Saskatchewan, Newfoundland and Labrador include a defence where conduct was 'incidental to the exercise of a lawful right of defence of person or property';[41] while
- Manitoba includes a defence where

> the act, conduct or publication was reasonable, necessary for, and incidental to, the exercise or protection of a lawful right of defence of person, property, or other interest of the defendant or any other person by whom the defendant was instructed or for whose benefit the defendant committed the act, conduct or publication constituting the violation.[42]

11.39 The ALRC considers that a specific defence is unnecessary to protect investigations into potential fraud or misrepresentation. The Insurance Council of Australia proposed such a defence.[43] It is in the interests of all policy holders that insurers have safeguards against fraudulent claims. Where they have reasonable grounds for suspecting fraudulent conduct, they or others on their behalf may often carry out investigations that could be viewed as invasions of privacy. The defence that the conduct was required or authorised by law is wide enough to cover these circumstances. For example, such conduct may be authorised by the statutory scheme under which the risk is insured, as in s 116 of the *Motor Vehicle Compensation Act 1999* (NSW), which requires a licensed insurer to 'take all such steps as may be reasonable to deter and prevent the making of fraudulent claims'. Alternatively, such conduct may already be expressly or impliedly authorised by the contract between the insurer and the insured.

11.40 In addition, the ALRC considers that individuals or organisations that engage in such conduct may be protected from liability under the public interest balancing test recommended in Chapter 9. In that chapter, the ALRC recommends that 'the prevention and detection of crime and fraud' be included in a list of public interest factors to be considered by a court.

Necessity

Recommendation 11–3 The Act should provide for a defence of necessity.

---

40 A Canadian court dismissed this defence in *Watts v Klaemnt* (2007) BCSC 662, [31]. In that case, a judge held that interception, recording and publication of telephone calls went well beyond what could be regarded as incidental to the exercise of a lawful right of defence of persons or property.

41 *Privacy Act*, RSBC 1996, c 373 (British Columbia) s 2(2)(b); *Privacy Act*, RSS 1978, c P-24 (Saskatchewan) s 4(1)(b); *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador) s 5(1)(b).

42 *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 5(c).

43 Insurance Council of Australia, *Submission 15*.

11.41 The ALRC recommends a defence of necessity be available under the new tort to protect individuals and organisations from liability where they had a reasonable belief that their conduct in invading the plaintiff's privacy was necessary to prevent an imminent and greater harm,[44] and where that conduct was a reasonable response to the situation. This defence will usually arise where the conduct was a response to an imminent danger or emergency, but may also be based on a semi-permanent state of affairs, where no other action could reasonably be taken to prevent the harm. This defence should be in line with the common law defence of necessity.

11.42 The defence of necessity operates in existing areas of Australian tort and criminal law[45] and several stakeholders supported a defence of necessity.[46]

11.43 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.[47] This necessity may arise, for example, where an individual has indicated an intention to self-harm and mental health professionals or emergency services obtain or disclose private information. It may also arise where a doctor is called to a school and needs to reveal private information about a child's vaccination record or a contagious disease or condition in dealing with an urgent situation.

11.44 The Australian Subscription Television and Radio Association (ASTRA) argued that the defence should be formulated in the following way: that the conduct was 'considered by the person acting to be reasonably necessary to eliminate or reduce a possible health, safety or security risk to themselves or another person'.[48]

11.45 Guardian News and Media Limited and Guardian Australia noted that, while a defence of necessity would be unlikely to apply to media organisations, there may be some situations where such a defence may be required:

> There are nevertheless some times when the appropriate public or private body does not disclose information which it may be in the public interest to disclose in aid of public safety and the media discloses.[49]

11.46 Several stakeholders opposed the inclusion of a defence of necessity,[50] or were concerned at what conduct it might excuse. Australian Pork submitted that the inclusion of such a defence would mean 'that any person infringing the rights may do so on the basis of a value judgement rather than a legal or public good basis'.[51]

---

44 Balkin and Davis, above n 3, 150.

45 *R v Loughnan* [1981] VR 443 [448].

46 T Butler, *Submission 114*; ABC, *Submission 93*; J Chard, *Submission 88*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; News Limited and Special Broadcasting Service, Submission No 76 to DPM&C Issues Paper, 2011.

47 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.

48 ASTRA, *Submission 99*.

49 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

50 Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Australian Pork Ltd, *Submission 83*.

51 Australian Pork Ltd, *Submission 83*.

11.47 However, existing law on the defence of necessity indicates that the belief of the defendant as to the necessity of their actions must be reasonable.[52] It has been suggested that the same latitude should be given to someone acting out of necessity as is given to someone acting in self-defence: that is, it will not matter if their belief in the necessity is mistaken, as long as it is reasonable.[53]

11.48 In the new tort, as with other intentional torts, the defence of necessity may apply in both public and private settings. Public necessity may involve 'invading the rights of private individuals in order to protect the community at large',[54] such as taking action to prevent a fire spreading.

11.49 A defence of private necessity would operate when the defendant commits a tort towards the plaintiff in order to protect persons or property (either their own, or a third party's) against the threat of imminent harm.[55] It does not matter if the altruist fails to achieve the objective, as long as the attempt was reasonable:

> Everyone who acts reasonably in a real emergency for the purpose of saving the goods of another from damage or destruction, whether he derives or is likely to derive any pecuniary advantage from the action or not, or is fulfilling any legal obligation.[56]

11.50 In the context of medical emergencies, courts have explained the proper function of the defence of necessity as justifying the administering of emergency procedures where a patient is not capable of providing consent.[57]

11.51 Considerations relevant to the defence may also be relevant to whether the plaintiff had a reasonable expectation of privacy and in relation to the public interest test, but the ALRC considers that a complete defence of necessity should be available to defendants as in other torts. This will be particularly important for emergency services, law enforcement officers and health professionals.[58]

Consent

Recommendation 11–4	The Act should provide for a defence of consent.

52 Kit Barker et al, *The Law of Torts in Australia* (Oxford University Press, 2012) 63.
53 Ibid. This is in reference to *Ashley v Chief Constable of Sussex Police* [2008] 2 WLR 975.
54 Balkin and Davis, above n 3, [6.22].
55 Ibid. J Goudkamp argues that there is only public necessity and that private necessity is not a tort defence. He treats defence of others' property as a public justification: James Goudkamp, *Tort Law Defences* (Hart Publishing, 2013) 116.
56 *Proudman v Allen* [1954] SASR 336 [341] (Hannan AJ).
57 *Re F* [1990] 2 AC 1 [66].
58 The defence of necessity is not available where the defendant's negligence caused the situation: *Simon v Condran* [2013] NSWCA 338.

11.52 A defence of consent will provide protection and certainty to defendants where a plaintiff has provided consent to a particular act or conduct which would otherwise amount to a serious invasion of privacy.[59] Consent may be express or implied. To be valid as a defence to an intentional tort, it is not necessary that consent be 'fully informed', but it must be actual consent by a person capable of giving consent and must be freely given.[60]

11.53 In many instances, an individual will have manifested clear consent to conduct that may otherwise amount to a serious invasion of privacy. Like the defence of voluntary assumption of risk to a negligence claim, it reflects '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'.[61]

11.54 Consent is a defence to many intentional torts, including battery, trespass to land and defamation.[62] It is a defence to the new action of misuse of personal information in the United Kingdom (UK).[63] In actions for breach of confidence, consent to the release of an obligation of confidence may be either absolute or limited to certain recipients.[64]

11.55 The Victorian Law Reform Commission (VLRC) recommended that consent be a defence.[65] The NSWLRC, rather than including consent with other defences, recommended that express or implied consent would negate the cause of action:

> The function of clause [74(4) of the Draft Bill] is to deny plaintiffs an action that they may otherwise have mounted. It does so by making the issue of consent an essential element of the statutory cause of action, with the result that if there is consent, there is no invasion of privacy. While this puts the onus on the plaintiff to prove a negative (namely the absence of the plaintiff's consent), forcing the plaintiff to make his or her case on consent at the outset allows the court to test whether the action has merit before it proceeds further.[66]

---

59 Several stakeholders support a defence of consent: 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*; D Butler, *Submission 10*; I Turnbull, *Submission 5*.

60 Contractual consent and similar terms will be subject to contract law and consumer protection laws.

61 *Smith v Baker* 325 1981 AC.

62 Barker et al, above n 52, 36. There is some debate in relation to battery as to whether absence of consent is an element of the cause of action that must be established by the plaintiff, or whether consent is a defence, that must be pleaded and proved by the defendant. Barker et al, take the view that it is as a defence.

63 M Warby et al, *Tugendhat and Christie: The Law of Privacy and The Media* (OUP Oxford, 2011) [12.09].

64 Tanya Aplin et al, *Gurry on Breach of Confidence* (Oxford University Press, 2nd ed, 2012) [14.16].

65 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) recs 27(a) and 28(a).

66 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [5.51].

11.56 The formulation of consent as a defence is consistent with the approach in four Canadian provinces which have enacted a statutory cause of action and included consent as either a defence[67] or an exception.[68]

11.57 In the Discussion Paper, the ALRC proposed that a plaintiff's consent be included as a factor for a court's consideration of whether the plaintiff had a reasonable expectation of privacy.[69]

11.58 Although the ALRC agrees that the plaintiff's consent to the conduct is relevant to whether or not they had a reasonable expectation of privacy in the circumstances, the ALRC now considers that it is preferable for a plaintiff's *actual* consent to specific conduct to be treated as a complete defence.[70] This will provide greater certainty to defendants who may rely on having obtained a person's consent prior to engaging in the specified conduct.

11.59 Many industries and professional groups operate on the basis and necessity of participant consent, either as part of contracts or for voluntary services or licences, including banking and financial services; medical and allied health practitioners; and social media providers, including social networking and dating organisations. The National E-Health Transition Authority (NeHTA) explained that consent is central to the viability of online medical records.[71] Without a complete defence of consent, such bodies would be exposed to uncertain liability.

11.60 The issue of whether consent has been given can be complex. For instance, consent in some circumstances may be withdrawn, the scope of consent may be unclear, or consent may have been given to other behaviour of the defendant or to third parties for similar conduct, such as publishing similar or related information. The fact that a person has previously consented to *other* conduct of the defendant (not within the scope of the consent given), or of third parties, may be considered as part of the general circumstances that are relevant when determining whether the plaintiff had a reasonable expectation of privacy. However, the ALRC considers that if a defendant can prove, and the onus will be on the defendant to do so, that the plaintiff actually consented to the conduct that is the subject of the complaint, this should be a complete defence.

---

67 *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 5(a); *Privacy Act*, RSS 1978, c P-24 (Saskatchewan) s 4(a); *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador) s 5(a).

68 *Privacy Act*, RSBC 1996, c 373 (British Columbia) s 2(a).

69 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) Proposal 6–2(h). This proposal stated that '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 whether the plaintiff consented to the conduct of the defendant'.

70 The ABC submitted that, while it is appropriate to look at the issue of consent in considering actionability, it is also appropriate for consent to be included as a complete defence where it is relevant to the circumstances of a particular case: ABC, *Submission 46*.

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

Express and implied consent

11.61 Whether a plaintiff provided actual consent will be a matter of fact, which will depend on the construction of words and conduct. There are a number of conditions to be satisfied for the defence:

- Consent must be given by the person whose privacy has been invaded, or by an individual who has legal capacity to consent on their behalf.[72]
- Consent may be given expressly or inferred from conduct[73] and the absence of written consent a defendant can rely on oral evidence,[74] or conduct[75]or the circumstances.[76]
- Consent must be freely given: consent obtained by duress will not be deemed to be free consent.
- Consent must be to the particular disclosure or act complained of.[77] Consent will be ineffective when the conduct performed by a defendant is of a materially different nature to the conduct to which the plaintiff consented.[78] The plaintiff's consent must relate to the extent of actual publication.[79]

11.62 To be effective, consent need not be fully informed, in the sense that the plaintiff was told of all the risks and implications of the conduct before giving consent. It is sufficient if the plaintiff is advised and consents in broad terms to the conduct.[80]

11.63 In relation to the publication of private information, English courts have shown caution in implying consent from the fact that the plaintiff engaged in earlier publicity.[81] Passive non-objection is generally not sufficient to demonstrate implied consent in actions for breach of confidence in the UK.[82]

11.64 Whether there was implied, actual consent to an actual publication is a distinct question from the issue of whether the plaintiff had a reasonable expectation of privacy. The need to distinguish these issues may arise where the plaintiff had previously released or allowed similar information to enter the public domain. Courts

---

72 Warby et al, above n 63, [12.10]; Aplin et al, above n 64, [14.07].
73 *Giller v Procopets* (2008) 24 VR 1.
74 Aplin et al, above n 64, [12.06].
75 Implied consent will be found where there has been positive action by a plaintiff which involves disclosure of their private information to another party: *Prout v British Gas plc and Another* [1992] FSR 478, (Ford J). The court in this case held that an application for a patent may be regarded as an implied release of the information into the public domain. This case was referred to in Aplin et al, above n 64, [14.15].
76 *Halliday v Neville* (1984) 155 CLR 1, [6] (Gibbs CJ, Mason, Wilson and Deane JJ).
77 Balkin and Davis, above n 3, [6.5].
78 Ibid.
79 *Campbell v MGN Ltd* [2004] 2 AC 457, [73]–[75] (Lord Hoffman). Lord Hoffman was referring to *Peck v United Kingdom* [2003] ECHR 44 (28 January 2003). See also, Warby et al, above n 63, [12.15].
80 *Rogers v Whitaker* (1992) 175 CLR 479, [490] (Brennan, Dawson, Toohey and McHugh JJ). Failure to fully inform a person of the risks involved does not vitiate consent but may constitute breach of any legal duty of care.
81 Warby et al, above n 63, [12.09].
82 Ibid [12.12].

in UK tort actions for misuse of private information have stipulated that if an individual courts public attention, 'they have less ground to object to the intrusion which follows'.[83] However, there is increasing recognition that a more nuanced approach is appropriate than was arguably shown in older cases, and that the appropriate time to look at prior publicity or conduct is when determining whether the plaintiff had a reasonable expectation of privacy at the relevant time.[84]

11.65 The digital era raises particular concerns in respect of consent to the publication of information. Commentators have questioned whether consent in online interactions and communications can be considered free and informed.[85] Online contracts and terms and conditions for online services such as internet banking and social media sites are often long, complex and are prone to frequent revision. Terms and conditions are often 'bundled'[86] without clear explanation of their meaning and consequences.[87] A situation may arise where a plaintiff consented, by agreeing to broad terms and conditions, to general conduct: the question of whether the specific conduct comes within the consent given will be a matter for the courts to construe.

11.66 Other stakeholders highlighted the difficulty for people to understand the nature, extent and legal effect of consent in intimate partner situations, both in ongoing relationships and in circumstances where the relationship breaks down.[88]

11.67 The ALRC considers that Australian courts are experienced in determining the scope and validity of a plaintiff's consent, whether express or implied, to particular conduct in a range of factual circumstances, such as online interactions and intimate partner situations.

Onus of proof

11.68 By classifying consent as a defence, the ALRC intends that a defendant will bear the onus of proving that a plaintiff consented to the defendant's conduct.

11.69 The question of who bears the onus of proving that a plaintiff consented to physical conduct for the tort of battery is contentious in English and Australian civil law. The plurality of opinions was highlighted in *Marion's case* by McHugh J:

> In England, the onus is on the plaintiff to prove lack of consent. That view has the support of some academic writers in Australia but it is opposed by other academic writers in Australia. It is opposed by Canadian authority. It is also opposed by

---

83 A similar principle has been applied in breach of confidence cases: the court might hold that the information no longer has the quality of confidence if the plaintiff had previously spoken publicly about related matters: *Theakston v MGN Ltd* [2002] EMLR 398; *Lennon v News Group Newspapers Ltd* [1978] FSR 573; *Woodward v Hutchins* [1977] 1 WLR 760.

84 Warby et al, above n 63, 540. See, also, Ch 6.

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

86 Law Institute of Victoria, *Submission 22*.

87 Australian Privacy Foundation, *Submission 39*.

88 Women's Legal Centre (ACT & Region) Inc, *Submission 19*. This submission highlights the increasing incidence of 'revenge pornography' where an individual discloses a compromising, sexually explicit photograph of a former partner which was obtained consensually during their relationship. See, also, *Giller v Procopets* (2008) 24 VR 1.

> Australian authority. Notwithstanding the English view, I think that the onus is on the defendant to prove consent. Consent is a claim of 'leave and licence'. Such a claim must be pleaded and proved by the defendant in an action for trespass to land. It must be pleaded in a defamation action when the defendant claims that the plaintiff consented to the publication. The *Common Law Procedure Act 1852* also required any 'defence' of leave and licence to be pleaded and proved. However, those who contend that the plaintiff must negative consent in an action for trespass to the person deny that consent is a matter of leave and licence. They contend that lack of consent is an essential element of the action for trespass to a person. I do not accept that this is so. The essential element of the tort is an intentional or reckless, direct act of the defendant which makes or has the effect of causing contact with the body of the plaintiff. Consent may make the act lawful, but, if there is no evidence on the issue, the tort is made out. The contrary view is inconsistent with a person's right of bodily integrity. Other persons do not have the right to interfere with an individual's body unless he or she proves lack of consent to the interference.[89]

11.70 The ALRC considers that the defendant will be best placed to provide evidence and prove that the plaintiff consented to the conduct invading privacy. Consent is generally considered to be a defence to an invasion of privacy in the UK.[90]

11.71 Despite not bearing the legal onus, the plaintiff may bear a provisional or tactical burden in relation to consent.[91] However, this does not create a legal burden to disprove facts.[92] In other words, where consent is a defence, a plaintiff has a non-legal, tactical obligation to show they did not provide consent.

11.72 While the ALRC recommends that a defendant bear the legal onus of proving that a plaintiff consented to the invasion of their privacy, a plaintiff will clearly have a strategic onus of showing that that their consent did not extend to a defendant's specific conduct, and may need to plead facts in reply.[93]

Revocation and withdrawal of consent

11.73 The legal effect of a revocation or withdrawal of consent may be an important consideration in cases involving disclosure of private information, and particularly so in the digital era where online publications remain active indefinitely.

11.74 As a matter of law, it is clear that just as a person may consent expressly or impliedly to another's conduct, so they may expressly or impliedly revoke that consent,

---

89 *Secretary, Department of Health and Community Services v JWB and SMB (Marion's case)* (1992) 175 CLR 218, [5] (McHugh J). (Citations omitted).

90 Warby et al, above n 63. This is despite the position in battery cases: *Freeman v Home Office (No 2)* [1984] QB 524. The English Court of Appeal held that in actions for battery, the burden of providing absence of consent is on the plaintiff as the tort redresses the 'unconsented to intrusion of anotherS' bodily integrity'.

91 This is a 'tactical obligation to lead counter-evidence placed upon a party against whom evidence has been adduced': J D Heydon, LexisNexis, *Cross on Evidence*, Vol 1 (at Service 164) [7005].

92 Ibid [7015].

93 'A plaintiff ought not, in the statement of claim, anticipate the defence and plead so as to meet the anticipated defence. The defence might not take the course reflected in the statement of claim, and useless material might be introduced into the pleadings … The statement of claim is limited to stating whatever material facts and points of law are necessary to show that the plaintiff has a right to relief': Bernard Cairns, *Australian Civil Procedure* (Thomson Reuters (Professional) Australia, 8th ed, 2009) [7.100].

provided reasonable notice is given to the other party.[94] Generally speaking, consent may be withdrawn at any time before the relevant conduct, despite a plaintiff having provided prior express consent.[95] However, it appears that a person cannot withdraw consent and expect the other party to act upon that revocation immediately if it would be unreasonable in the circumstances to expect them to do so.[96]

11.75 To revoke a consent given under contract—for example, for the publication of certain information or to appear on a television program—may of course be a breach of that contract. However, the other party would be entitled to damages, assessed on the usual basis, and should not be disentitled to revoke their consent. It would be difficult for the other party to obtain relief by either the equitable remedy of specific performance of the contract, or an injunction to restrain the (probably implied) promise not to breach it. Most cases would involve the media or other commercial publishers for whom damages would usually be adequate to remedy the harm done by the breach (either expense wasted in reliance on the contract going ahead or loss of the profits expected).[97]

11.76 In the UK, there is limited authority on the circumstances in which consent to the use or disclosure by the media of an individual's private information may be revoked.[98] Copyright law can provide some guidance here. A licence which is provided gratuitously can be revoked with notice at any time in circumstances where no stipulation for its duration has been made.[99]

11.77 In the privacy context, there are some other scenarios where the effect of revocation of consent will not be straightforward. One would be the online disclosure of personal information by a defendant, with the plaintiff's consent, during the course of an intimate relationship, which has subsequently ended and where the plaintiff no longer wants the information to be available to others. Another would be where a person has gratuitously consented to the publication of private facts by a journalist and then wishes to revoke the consent.

11.78 Subject to public interest matters, a revocation may certainly be effective to control future disclosures or publications. It would not be effective to counteract a publication, based on the consent that has already happened, such as in a book, magazine, newspaper or documentary film.

11.79 Another area of uncertainty is where prior consent was given to a publication of information, in the nature of a continuing publication. In a sense, all information available online is continually published: publication occurs every time the information is downloaded from a website.[100] So the question arises as to whether a person can

---

94 *Cowell v Rosehill Racecourse Co Ltd* [1937] ALR 273.
95 Balkin and Davis, above n 3, [6.13].
96 This seems the better explanation, in modern times, for cases like *Herd v Weardale Steel Coal and Coke Co Ltd* [1915] AC 67. See also, Barker et al, above n 52, 79.
97 See further JW Carter, *Contract Law in Australia* (Lexis Nexis Butterworths, 6th ed, 2013) ch 40.
98 Warby et al, above n 63, [12.19].
99 Ibid.
100 *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575.

effectively revoke actual consent that was given before or at the time of the posting, ask for the posting to be taken down, and if it is not, successfully assert that the *continuing* publication is a serious invasion of privacy.[101] If the plaintiff's actual consent is the only fact stopping the publication being an invasion of privacy, then it is arguable that the revocation should be effective. However, there are likely to be other considerations. While this issue will no doubt be argued, in Australia or elsewhere, the issue as it applies to privacy law is somewhat hypothetical and uncertain.[102]

11.80 The ALRC suggests that the best way to approach this issue would be to deal with it as part of the question of whether or not the plaintiff has a reasonable expectation of privacy at the time of the action, taking into account the revocation of prior consent, the reasonableness of the revocation and of the request for the posting to be taken down, the reasonableness or otherwise of the defendant's refusal or failure to do so, and the public interest in its continuing publication.[103]

Absolute privilege

Recommendation 11–5 The Act should provide for a defence of absolute privilege.

11.81 The ALRC recommends that the defence of absolute privilege[104] be available as a defence to the new tort to protect defendants from liability when their communications arise in a particular context.[105] 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.[106]

---

101 It should be noted that this scenario does not involve information posted by others without the subject's consent, which is another scenario raising the contentious and topical issue of whether there is some legal 'right to be forgotten', discussed in Ch 16.

102 Warby et al, above n 63, 537–538.

103 See Ch 6

104 Several stakeholders supported the availability of this defence under the new privacy tort: N Witzleb, *Submission 116*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; Australian Bankers' Association, *Submission 84*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; N Witzleb, *Submission 29*.

105 The ALRC and the VLRC previously recommended a defence of privilege to a statutory cause of action: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) rec 74–4(c); Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) rec 27(e).. 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: Telstra, *Submission 107*; NSW Young Lawyers, *Submission 58*; ABC, *Submission 46*; Arts Law Centre of Australia, *Submission 43*; Law Institute of Victoria, *Submission 22*; D Butler, *Submission 10*.

106 Legislation provides a non-exhaustive list of occasions which attract absolute privilege, for eg, *Defamation Act 2005* (NSW) 2005 s 27.

11.82 The ALRC considers that this defence should be co-extensive with the defence of absolute privilege to defamation, so that it includes both statutory and common law defences of absolute privilege,[107] and so that the same principles would apply whether an action is brought for defamation or invasion of privacy by publication of private information. The rationale of absolute privilege is equally applicable to both actions.

11.83 For example, under s 27(2) of the *Defamation Act 2005* (NSW), a statement is published on an occasion of absolute privilege if:

> (a) the matter is published in the course of the proceedings of a parliamentary body, including (but not limited to):
>
> (i) the publication of a document by order, or under the authority, of the body, and
>
> (ii) the publication of the debates and proceedings of the body by or under the authority of the body or any law, and
>
> (iii) the publication of matter while giving evidence before the body, and
>
> (iv) the publication of matter while presenting or submitting a document to the body, or
>
> (b) the matter is published in the course of the proceedings of an Australian court or Australian tribunal, including (but not limited to):
>
> (i) the publication of matter in any document filed or lodged with, or otherwise submitted to, the court or tribunal (including any originating process), and
>
> (ii) the publication of matter while giving evidence before the court or tribunal, and
>
> (iii) the publication of matter in any judgment, order or other determination of the court or tribunal, or
>
> (c) the matter is published on an occasion that, if published in another Australian jurisdiction, would be an occasion of absolute privilege in that jurisdiction under a provision of a law of the jurisdiction corresponding to this section, or
>
> (d) the matter is published by a person or body in any circumstances specified in Schedule 1.

11.84 This defence recognises the importance of protecting certain communications or statements from liability in the interests of free speech and transparency. Rigorous debate in such proceedings may reveal personal information. Privilege in this context can be understood as a necessary restriction on privacy interests in a democratic society.

11.85 Wiztleb supported this principle, stating that

> the underlying rationale of all these defences is that a person should in that particular context be able to communicate freely and without fear of incurring civil liability …

---

107 See, 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.

> The privilege has the purpose of protecting and facilitating frank and fearless communication even if it is damaging to reputations because it is considered in the public interest to do so. This same reasoning can also be applied to the protection of privacy. It is therefore appropriate to create privileges for communications in which this rationale applies.[108]

11.86 In the defamation case, *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.[109] This defence facilitates Australia's democratic system by enabling the free and fair exchange of debate in certain circumstances and which may involve the disclosure of an individual's private information.

11.87 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 from liability.[110]

11.88 Defences of privilege operate in Canadian privacy statutes.[111]

Publication of public documents

Recommendation 11–6 The Act should provide for a defence of publication of public documents.

11.89 This defence provides protection from liability for the publication of public documents which are relevant to an open and transparent political and legal system. Access to public documents supports the principle of open justice and accountability in our public institutions. This recommendation is consistent with the ALRC's Terms of Reference for this Inquiry which require consideration of the necessity of balancing privacy with fundamental values, including freedom of expression and open justice.

11.90 The ALRC recommends that this defence should be co-extensive with the defence of publication of public documents in s 28 of the Uniform Defamation Law (UDL) which provides a comprehensive list of the types of documents protected from defamation actions.[112] The use of this list will dispel any concerns about the scope of the defence by clearly defining the range of documents covered by the defence. Section 28 defines 'public document' as

---

108 N Witzleb, *Submission 29*.

109 *Mann v O'Neill* (1997) 191 CLR 204, 212 (Brennan CJ, Dawson, Toohey and Gaudron JJ).

110 *Parliamentary Privileges Act 1987* (Cth) s 16 and parallel state acts. See, Butler and Rodrick, above n 34, [3.700].

111 *Privacy Act*, RSBC 1996, c 373 (British Columbia) s 2(b).

112 The application of this provision in the new privacy tort was supported by the Office of the Victorian Privacy Commissioner, *Submission 108*.

(a) any report or paper published by a parliamentary body, or a record of votes, debates or other proceedings relating to a parliamentary body published by or under the authority of the body or any law, or

(b) any judgment, order or other determination of a court or arbitral tribunal of any country in civil proceedings and including:

(i) any record of the court or tribunal relating to the judgment, order or determination or to its enforcement or satisfaction, and

(ii) any report of the court or tribunal about its judgment, order or determination and the reasons for its judgment, order or determination, or

(c) any report or other document that under the law of any country:

(i) is authorised to be published, or

(ii) is required to be presented or submitted to, tabled in, or laid before, a parliamentary body, or

(d) any document issued by the government (including a local government) of a country, or by an officer, employee or agency of the government, for the information of the public, or

(e) any record or other document open to inspection by the public that is kept:

(i) by an Australian jurisdiction, or

(ii) by a statutory authority of an Australian jurisdiction, or

(iii) by an Australian court, or

(iv) under legislation of an Australian jurisdiction, or

(f) any other document issued, kept or published by a person, body or organisation of another Australian jurisdiction that is treated in that jurisdiction as a public document under a provision of a law of the jurisdiction corresponding to this section, or

(g) any document of a kind specified in Schedule 2.[113]

11.91 The NSWLRC argued that the consideration of public interest in its public documents and fair report of proceedings of public concern.[114] However, a complete defence would provide greater certainty.

11.92 A number of stakeholders expressed their support for the availability of this defence, many of whom highlighted the need to promote a transparent and open government and judicial system.[115]

113 See, for example, *Defamation Act 2005* (NSW) 2005 s 28(4).

114 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.8].

115 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; ASTRA, *Submission 99*; Australian Sex Party, *Submission 92*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; SBS, *Submission 59*; D Butler, *Submission 10*.

Fair report of proceedings of public concern

Recommendation 11–7 The Act should provide for a defence of fair report of proceedings of public concern.

11.93 This recommendation provides a defence for individuals who publish or otherwise disclose fair reports of public proceedings which may, in the process, reveal an individual's private information. This defence will be of particular significance for media organisations, court reporters and educational institutions.

11.94 The ALRC recommends that this defence should be co-extensive with the defence of fair report of proceedings of public concern in the UDL.[116] This statutory defence applies to the publication of defamatory matter contained in documents from proceedings of a parliamentary body, an international organisation, court or tribunal, inquiries including Royal Commissions, meetings of shareholders of a public company, and other public proceedings as outlined in the relevant provision of the UDL.

11.95 The ALRC considers that the meaning of 'fair', as it has developed at common law and in the interpretation of the UDL, should apply to this recommendation. At common law, 'fair' refers to summaries of proceedings which intend to honestly convey to the reader the impression which the proceedings would have had if the reader had been present.[117] Whether a report is fair will be a question of fact for a court, to be determined objectively by comparing the report to the events or facts it described. The impression conveyed in the report must not be substantially different from the impression that someone would have gleaned had they been present at the relevant event.[118]

11.96 Several stakeholders supported this defence.[119] While the National Association for the Visual Arts (NAVA) supported the availability of the defence, it argued that it should be expanded to include artistic representations.[120] However, the ALRC considers that artistic expression is more appropriately considered in the public interest balancing test which is part of the actionability for the cause of action.

11.97 Stacey Higgins argued that the defence is unnecessary as publications which are already in the public domain will not be subject to liability.[121] The ALRC has recommended in Chapter 6 that, whether the material was already in the public domain should be taken into account when determining whether the plaintiff had a reasonable

116 See, for example, *Defamation Act 2005* (SA) 2005 s 29(4).
117 *Bashford v Information Australia (Newsletters) Pty Ltd* (2004) 218 CLR 366; *Cook v Alexander* [1974] 1 QB 279; *Rogers v Whitaker* (1992) 175 CLR 479.
118 *Waterhouse v Broadcasting Station TGB Pty Ltd* (1985) 1 NSWLR 58, [62]–[63].
119 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; ASTRA, *Submission 99*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*.
120 National Association for the Visual Arts Ltd, *Submission 78*.
121 S Higgins, *Submission 82*.

expectation of privacy. However, the ALRC considers that the interests of open government, transparency and open justice require a complete defence.

11.98 The Public Interest Advocacy Centre (PIAC) argued that the publication of material which is already in the public domain, including public documents and reports of proceedings, should not be protected by a defence, as the publication of private information which is already publicly available can cause distress:

> the collection, use and disclosure of information about a person from publicly available sources can still have considerable privacy impacts. For example, information in the public domain would arguably include press clippings, which might contain inaccurate information, or accurate information that is open to misinterpretation. Information may still be private and personal to the plaintiff, despite the fact that it has been published, or is contained in a public record (for example, a person's criminal record, their HIV status, or the fact that they are a rape victim).[122]

11.99 The ALRC considers that this concern is addressed by the inclusion of the explanation that the defence is co-extensive with the defence to defamation. The definition of public documents in s 29 of the UDL provides a clear list of the proceedings which are subject to this defence. It also provides that the defence may be defeated if the matter was not published honestly for the information of the public or the advancement of education. The publication of some private information that is revealed in the course of open proceedings is also the subject of other specific legislation such as *Judicial Proceedings Acts* in the states and territories that prohibit the publication of private information in certain court proceedings. This includes the identity of protected classes of people such as jury members, children and the victims of sexual assault.[123] Publication would also be subject to any suppression order of the court.[124]

Safe harbour scheme for internet intermediaries

11.100 Internet intermediaries[125] should not be liable under the tort for invasions of privacy committed by third parties using their services, where they have no knowledge

---

122 Public Interest Advocacy Centre, *Submission 105*.

123 See, eg, the *Judicial Proceedings Report Act 1985* (Vic). Provisions in this Act restrict the publication of certain information in specific judicial proceedings.

124 See, eg, *Court Suppression and Non-Publication Orders Act 2010* (NSW) s 8. This provision empowers a court to make a suppression order 'where the order is necessary to avoid causing undue distress or embarrassment to a party to or witness in criminal proceedings involving an offence of a sexual nature (including an act of indecency)'.

125 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. There is also a comprehensive definition of 'carriage service provider' in the *Telecommunications Act 1997* (Cth) s 87. For the purposes of that Act, the provision defines a 'listed carriage service provider' as someone who provides carriage service to the public using a network owned by one or more carriers. This definition excludes online search engines and online vendors as they provide a platform for their customers, but not for the *public*. This definition restricts the scope of the safe harbour scheme.

of the invasion of privacy. Where they do have knowledge, there does not seem to be any justification to provide a complete exemption from liability. The ALRC therefore sees no need to recommend the enactment of a 'safe harbour' scheme, to protect internet intermediaries from liability under the tort.

11.101 There are two reasons why intermediaries are unlikely to be liable under this tort. First, the tort is targeted at positive conduct on the part of the defendant. It is difficult to characterise a failure to act as an 'invasion' of privacy. It is not intended to impose liability for mere omissions—that is, failing to act to stop an invasion of privacy by a third party.[126] Secondly, the tort is confined to intentional or reckless invasions of privacy.

11.102 A mere intermediary will rarely have this level of intent, when third parties use their service to invade someone's privacy. The operators of a social networking platform, for example, do not intend to invade someone's privacy, when one of its customers posts private information about another person on the platform.

11.103 In some circumstances, an intermediary *may* be found to have the requisite fault after they have been given notice of an invasion of privacy. They may be found to have intended an invasion of privacy, or been reckless, if they know that their service has been used to invade someone's privacy, and they are reasonably able to stop the invasion of privacy, but they choose not to do so.[127]

11.104 Considering these two reasons, the ALRC does not think it necessary to recommend that safe harbour schemes for internet intermediaries be extended to protect intermediaries from liability under the new tort.

11.105 However, if such a scheme were necessary, amending cl 91 of sch 5 of the *Broadcasting Services Act 1991* (Cth) may be one way of protecting intermediaries from liability under the tort. Clause 91 does not currently refer to laws under Commonwealth statutes. It provides that any law of a state or territory, or a rule of common law or equity has no effect to the extent to which it subjects an internet content host to liability in respect of hosting particular internet content.[128]

11.106 In copyright law, s 116AG of the *Copyright Act 1968* (Cth) limits the remedies a court may grant against carriage service providers for infringements of copyright that relate to their carrying out certain online activities. In order to access this scheme, a carriage service provider must meet conditions in s 116AH.

---

126 Defamation is not limited to positive conduct in this way. The Court of Appeal of England and Wales, in *Byrne v Deane*, found the proprietors of a golf club liable for defamation, when someone anonymously posted a defamatory poem to the wall of the club. The club knew the defamatory poem was posted on the wall and could have taken it down, but did not: *Byrne v Deane* [1937] 1 KB 818. This principle has been applied to hold internet intermediaries liable as publishers in defamation where they have been given notice of defamatory matter present on their website, but fail to remove it within a reasonable time: *Godfrey v Demon Internet Ltd* [2001] QB 201; *Tamiz v Google Inc* [2013] 1 WLR 2151; *Trkulja v Google Inc LLC* [2012] VSC 533; *Rana v Google Australia Pty Ltd* [2013] FCA 60.

127 *Byrne v Deane* [1937] 1 KB 818.

128 *Broadcasting Services Act 1992* (Cth) Sch 5 cl 91(a).

11.107 In the Discussion Paper, the ALRC proposed the introduction of a safe harbour scheme, to protect internet intermediaries from liability under the new tort for which a third party was primarily responsible.[129] To rely on the defence, the intermediary might be required to meet certain conditions. The defence would not apply to invasions of privacy that intermediaries themselves intentionally or recklessly commit.

11.108 In the US, § 230 of the *Communications Decency Act 1996* (US) contains a broad safe harbour scheme.[130] The scheme exempts 'interactive computer services' from civil liability under US state and federal law where

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). [131]

11.109 The provision also imposes a series of obligations on interactive computer service providers:

> A provider of an interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.[132]

11.110 The EU safe harbour scheme provides that service providers are not under any 'general obligation to monitor' for illegal content.[133] Services will not be liable for third party content where the internet intermediary had no 'actual knowledge of illegal activity or information knowledge' and, 'upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information'.[134]

11.111 In the UK, the *Defamation Act 2013* (UK) provides a defence for 'operators of websites'.[135] It is a defence for the operator to show that it was not the operator who posted the statement on the website.[136] An operator of a website is understood as a

---

129 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.

130 M Lemley, 'Rationalizing Internet Safe Harbors' (2007) 6 *Journal on Telecommunications and High Technology Law* 101, 102.

131 *Communications Decency Act 1996, Title V of the Telecommunications Act 1996, 47 USC*.

132 Ibid s 230(c)(d).

133 *EU Directive on Electronic Commerce* (2000/31/EC) art 15.

134 Ibid art 14.

135 *Defamation Act 2013* (UK) s 5. This defence is defeated if the defendant showed malice: Ibid s 5(11). The Explanatory Memorandum to the Act explain that malice may arise in circumstances where the operator of a website had 'incited the poster to make the posting or had otherwise colluded with the poster': Explanatory Notes, Defamation Bill 2013 (UK) [42].

136 *Defamation Act 2013* (UK) s 5(2).

person with effective control over the content of a website who is not the author, editor or publisher of the matter. There are differing degrees of control depending on the form and size of a platform.

11.112 Section 5(12) provides that the act of merely 'moderating' a site is not, in and of itself, sufficient to defeat the defence.

11.113 The defence is defeated if the claimant shows that

> (a) it was not possible for the claimant to identify the person who posted the statement,
>
> (b) the claimant gave the operator a notice of complaint in relation to the statement, and
>
> (c) the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.

11.114 The provision sets out in some detail the scope of UK privacy regulations[137] that an internet service provider must adhere to, as well as the nature of a complaints system.[138]

11.115 This detailed defence is complemented by s 10 which provides that a court does not have jurisdiction to hear and determine an action for defamation brought against a person who was not the author, editor or publisher of the statement complained of unless the court is satisfied that it is not reasonably practicable for an action to be brought against the author, editor or publisher.

Conditions

11.116 If a safe harbour scheme were enacted, internet intermediaries should be required to comply with certain conditions to rely on the defence. Examples of such conditions might include requiring internet intermediaries to

- 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; and
- comply with relevant industry codes and obligations under the *Privacy Act 1988* (Cth).

11.117 Stakeholders suggested other conditions, including requiring internet intermediaries to

- reasonably cooperate with and assist the relevant regulator with locating and pursuing a wrongdoer;[139]

---

137 Ibid s 5(5).
138 Ibid s 5(6).
139 Office of the Australian Information Commissioner, *Submission 90*.

- take action against individuals who are found liable for serious invasion of privacy, such as blocking their social media accounts;[140]
- block users who contravene these terms and conditions from uploading future content;[141] and
- show warnings about the risks and potential consequences of posting private information.[142]

11.118 While the ALRC recommends that a safe harbour scheme is unnecessary, if such a defence were to be enacted consideration should be given to these conditions.

Exemption or defence for children and young persons

Recommendation 11–8 The Act should provide for an exemption for children and young persons.

11.119 The ALRC recommends that the statutory cause of action should contain an exemption or defence where the invasion of privacy occurred when the defendant was a child or a young person under an age to be specified by the legislature.

11.120 This defence was not proposed in the Discussion Paper and the ALRC has not therefore received stakeholder comments. The ALRC nevertheless makes this recommendation in this Report, for a number of reasons.

11.121 In the digital era there is a significant potential for a child or a young person to misuse digital communications technology to invade the privacy of another child or young person while joining in with increasingly common forms of behaviour and social interaction. Although the ALRC recognises that substantial emotional distress may be caused by an invasion of privacy committed by a child or young person, the ALRC considers that education on the risks and ethical dimensions of such behaviour is more appropriate than the imposition of civil liability on children and young people below a specified age.

11.122 Available research indicates that age is a factor in how children and young people navigate online spaces.[143] Age plays a role in the risks that young people face, the risks they are willing to take, and in their understanding of the implications of the risks, from engaging in online platforms and other communications using apps and mobile phones. Research indicates that young people are generally aware of privacy

140 Women's Legal Services NSW, *Submission 115*.
141 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*.
142 S Higgins, *Submission 82*. Other stakeholders also recommended possible conditions: UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Sex Party, *Submission 92*; Interactive Games and Entertainment Association, *Submission 86*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*.
143 B Nansen et al, 'Children and Digital Wellbeing in Australia: Online Regulation, Conduct and Competence' (2011) 6 *Journal of Children and Media* 237, 237.

risks associated with some behaviour, such as sexting.[144] However this awareness varies significantly—and perhaps unsurprisingly—depending on their age and capacity.

11.123 Given the increased affordability, capacity and usage of digital and mobile technology, children and young persons may therefore be more likely than in previous eras to engage in intentional or reckless behaviour which could expose them to liability under the new tort.

11.124 At common law, a child or young person can be liable in tort. There are rare examples of successful action in the case of personal injury inflicted by a child.[145] Negligence law takes account of the age of a child in determining the standard of care that can be expected of a child of a similar age, experience and level of intellectual development.[146] There is usually no point suing children or young people where the injury is minor or because of their lack of assets, but different considerations apply if the conduct caused lasting or significant injury and if liability for negligence is covered by household or other insurance policies.

11.125 For intentional torts, a child must be of sufficient age to form the relevant intent. This principle would be relevant to the new tort if the recommended defence were not included.

11.126 Unlike liability for negligence, insurance does not usually cover liability for intentional wrongs, so there may be little point suing a minor at the time. Liability for a tort endures until the expiration of the relevant limitation period, which in the case of a plaintiff who is a minor may be some years after the conduct. The ALRC considers it would be undesirable for the legislation to allow a young person to be sued for something done, potentially, years before when they were under the specified age.

11.127 Parents of a child who has committed a tort are not vicariously liable to the plaintiff for the child's conduct. They can be liable if their lack of supervision amounts to a breach of their own duty of care in negligence to supervise or control their child,[147] or if they have failed to secure goods to which the child should not have had access, particularly dangerous goods.[148] Liability in negligence only arises where the plaintiff suffers actual damage. As the new tort of invasion of privacy is limited to intentional or reckless conduct, negligence by a parent in supervising a child would not give rise to liability under the new tort.

---

144 S Walker, L Sanci and M Temple-Smith, 'Sexting: Young Women's and Men's Views on Its Nature and Origins' (2013) 52 *Journal of Adolescent Health* 697.

145 Balkin and Davis, above n 3, 830.

146 Twelve year old not liable in negligence for throwing a dart which hit the plaintiff child in the eye: *McHale v Watson* (1964) 111 CLR 384.

147 *Smith v Leurs* (1945) 70 CLR 256; *Curmi v McLennan* [1994] 1 VR 513.

148 Plaintiff injured in eye by another teenager using an airgun after defendant had left it in an unlocked cupboard on a houseboat which he allowed his teenage son and friends to occupy: *Curmi v McLennan* [1994] 1 VR 513.

11.128 Standards and provisions in other legislation provide a useful model for legislators when considering an appropriate age at, or under which, liability under the new tort should not exist.

11.129 Commonwealth criminal law provides that a child under 10 years of age cannot be liable for a criminal offence.[149] A child aged between 10 and 14 will only be liable if that child knows their conduct is wrong.[150] Other legislation assumes differing levels of understanding and capacity depending on a young person's age, for example, in NSW, the consent of a young person over the age of 14 years is effective consent to medical treatment to prevent which would otherwise be a battery.[151]

11.130 There is evidence in recent Australian literature and government inquiries that legislatures and others are concerned about criminalising the behaviour of children and young persons, with long term effects on a young person's record of behaviour. A number of other recent or current inquiries are being conducted into the age at which young people should be held liable for offences involving the use of communications networks or other criminal offensive or harmful behaviour.[152]

11.131 The ALRC recommendation does not specify an age under which a young person should not be liable but suggests that it should be consistent with other legislation reflecting analogous rationales. The ALRC's tentative view is that 16 would be an appropriate age under which a young person should not have a civil liability.

Defences unsuited to a privacy action

Other defamation defences

11.132 The ALRC considers that some defences to defamation are inappropriate or unnecessary for a privacy action, due to the differences in the nature, rationale and elements of the two causes of action.

11.133 **Truth.** The defence of truth or justification[153] 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.

11.134 **Fair comment.** A defence of fair comment[154] is inappropriate for a privacy tort. The right to speak freely, that is protected by the defence of fair comment in defamation law, both under common law and the UDL, is limited to comment or opinions on matters of public interest. In the new tort, public interest will already have been considered as part of actionability, so that a defence is unnecessary. Further, the relevant wrong in the invasion of privacy tort is the disclosure of private information.

---

149 *Crimes Act 1914* (Cth) s 4M.
150 Ibid s 4N(1).
151 See, eg, *Minors (Property and Contracts) Act 1970* (NSW) s 49(2).
152 For example, the Victorian Parliament's Law Reform Committee undertook an inquiry into sexting in 2013 that considered the impact of legislation that criminalises consensual criminalising sexting on minors: Parliament of Victoria Law Reform Committee, 'Report of the Law Reform Committee for the Inquiry into Sexting' (Parliamentary Paper 230, 2013).
153 See, for example, *Defamation Act 2005* (NSW) 2005 s 25.
154 *Privacy Act*, RSBC 1996, c 373 s 2 includes the defence of fair comment.

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.[155]

11.135 **Qualified privilege.** The ALRC has decided not to recommend a defence akin to that of qualified privilege in defamation law. Qualified privilege at common law protects defamatory statements where they are made without malice on an occasion of qualified privilege, that is, where a person has a legal, social or moral duty or interest in making the statement to someone with a reciprocal duty or interest in receiving it. The defence is lost if the defendant was actuated by an improper motive. The common law defence very rarely benefited the media, who had instead to rely on extended statutory or constitutional forms of the defence.[156] Although a defence similar to qualified privilege at common law was discussed and proposed in the Discussion Paper,[157] and some stakeholders supported it,[158] other expert commentators and legal practitioners, in consultations with the ALRC, questioned the need for or desirability of such a defence, given the elements of the cause of action and other defences.[159]

11.136 A number of considerations underpin the ALRC's decision not to recommend a defence of qualified privilege. First, the new tort would apply only to intentional or reckless invasions of privacy, so there is a need for compelling reasons to justify the invading conduct. Defamation, by contrast, is a tort of strict liability, therefore necessitating a greater range of defences for conduct in good faith to alleviate the potential harshness of the liability.

11.137 Secondly, commentators also pointed to the fact that complex questions arise as to the elements and operation of qualified privilege in defamation law. If there were a need for a similar defence to the common law defence, it would be undesirable to burden the new tort with that complexity and risk extended legal argument about how common law principles relevant to the defamation defence applied to the new tort. An

---

155 N Witzleb, *Submission 29*. The VLRC recommended a defence of fair comment but such a defence was not recommended by the ALRC previously or by the NSWLRC. NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [6.8]; Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) rec 27(e).

156 As set out in Discussion Paper 80 at [10.40]—[10.52], there are three categories of qualified privilege in defamation: qualified privilege at common law, qualified privilege under the UDL (see, eg, s 30 in the *Defamation Act 2005* (NSW)) and the *Lange* qualified privilege encompassing implied freedom of political communication.

157 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014).

158 Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Telecommunications Industry Ombudsman, *Submission 103*; ASTRA, *Submission 99*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; Telstra, *Submission 45*; N Witzleb, *Submission 29*.

159 Office of the Information Commissioner Queensland, *Submission 127*; Public Interest Advocacy Centre, *Submission 105*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Australian Privacy Foundation, *Submission 39*; T Gardner, *Submission 3*. The ALRC considers that the requirement for the plaintiff to have a reasonable expectation of privacy, the fault element of intentional or reckless conduct, the public interest balancing process as part of actionability and the defence of reasonable defence of persons, others or property will provide overall sufficient protection to conduct that would fall within a defence of qualified privilege.

entirely new defence would need to be drafted to deal with the situations intended to be protected.

11.138 Thirdly, a plaintiff would arguably not satisfy the actionability requirements for bringing an action in any of the circumstances that would attract the defence. Where a defendant acted in circumstances commonly included within occasions of qualified privilege at common law, the plaintiff would not usually have a reasonable expectation of privacy in relation to the information. Alternatively, any invasion of privacy would arguably be outweighed by public interest considerations relating to the circumstances.[160] Lastly, the defences of necessity or defence of persons or property may excuse the defendant. If not, an intentional and reckless invasion of privacy should be actionable.

11.139 **Innocent dissemination.** The defence of innocent dissemination[161] is inappropriate, as the statutory cause of action is limited to intentional acts. While several stakeholders supported the inclusion of a defence of innocent dissemination, this may have been on the basis that the fault elements of the action were not confirmed at that time.

11.140 Innocent dissemination is a defence to defamation in which liability is strict. A defendant has the defence if they published the defamatory material merely in the capacity of a 'subordinate distributor', and neither knew, nor ought reasonably to have known, that the matter was defamatory.[162] The defence of innocent dissemination may be considered a type of safe harbour.[163]

11.141 **Triviality.** The defence of triviality is unnecessary as the statutory cause of action is confined to *serious* invasions of privacy.[164]

11.142 **Information in the public domain.** The ALRC considers that a complete defence of 'information in the public domain'—or the application of the doctrine of waiver[165]—would be inappropriate, as the effect of a prior disclosure of an individual's (prima facie) private information is variable.

11.143 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.[166]

---

160 Witzleb notes that: 'The privilege has the purpose of protecting and facilitating frank and fearless communication even if it is damaging to reputations because it is considered in the public interest to do so. This same reasoning can also be applied to the protection of privacy. It is therefore appropriate to create privileges for communications in which this rationale applies': N Witzleb, *Submission 29*.

161 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.

162 See, eg, *Defamation Act 2005* (NSW) 2005 s 32.

163 Leonard, above n 125, 235.

164 SBS, above n 21 supported the availability of the defence of triviality.

165 Warby et al, above n 63, 539–542.

166 Public Interest Advocacy Centre, *Submission 30*.

11.144 Several stakeholders supported the inclusion of a defence that the information disclosed by the defendant was already in the public domain.[167]

11.145 However the ALRC recommends that, whether and to what extent information is in the public domain at the relevant time, as well the plaintiff's prior conduct in having a role in the earlier disclosure, will be a relevant factor to be considered by a court when determining whether a plaintiff had a reasonable expectation of privacy. This factor is discussed more fully in Chapter 6.

11.146 In making this recommendation, the ALRC recognises that there may be some circumstances where the previous widespread dissemination of an individual's private information may diminish their reasonable expectation of privacy, even if the facts do not support implied consent to that publication.[168] On the other hand, the fact that private information was once publicly or broadly known may not justify the defendant's revealing it at a later time. These matters are best considered by the court when determining whether the plaintiff has a cause of action.[169]

11.147 **Public interest.** A defence of public interest would be redundant because the ALRC recommends in Chapter 9 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 any countervailing public interest. A separate public interest defence would therefore not be needed.[170]

11.148 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. The balancing of public interests is discussed more fully in Chapter 9.

Contributory negligence

11.149 A defence of contributory negligence is not appropriate for the new tort, which is limited to intentional or reckless conduct. This approach is consistent with the law relating to other intentional torts, such as conversion, battery and assault.[171]

11.150 Opening the new privacy tort up to defendant claims of contributory negligence would confuse the fault element of the tort by introducing consideration of negligent conduct. Contributory negligence now acts as a partial defence only to claims

---

167 SBS, *Submission 59*; ABC, *Submission 46*; D Butler, *Submission 10*; T Gardner, *Submission 3*.

168 See the discussion of the defence of consent above.

169 This is also the case in breach of confidence actions where information must have the quality of confidence to be protected in equity. This may be lost if the information becomes known to a substantial number of people. Contractual obligations of confidence may endure even where the information has been publicly revealed. See, further, Aplin et al, above n 64, ch 5.

170 Several stakeholders supported this model: Office of the Australian Information Commissioner, *Submission 66*; Google, *Submission 54*; ASTRA, *Submission 47*; ABC, *Submission 46*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*.

171 Cf *New South Wales v Riley* (2003) 57 NSWLR 496, [104].

in negligence, and statute authorises the reduction of damages where the plaintiff's own negligence was a material factor in the loss or harm suffered.[172]

11.151 The ALRC considers that, where a defendant intentionally or recklessly and unjustifiably invades another person's privacy, and cannot rely on one of the available defences, such conduct should not be excused or mitigated by mere carelessness on the part of the plaintiff. The plaintiff's conduct may be a consideration when the court is deciding whether the plaintiff had a reasonable expectation of privacy.

Other defences and exemptions

11.152 The ALRC considers that, other than in the case of young people, no activity, individual or organisation should be exempt from liability under the new tort. A number of stakeholders agreed, arguing that defences would be sufficient to protect serious invasions of privacy which are nonetheless warranted.[173]

11.153 Other stakeholders raised a number of other possible exemptions or defences to the new tort. However, the ALRC considers that many of these are appropriately captured by the recommended defences, such as lawful authority or necessity, or by the elements of the tort, including the requirement of a reasonable expectation of privacy and the public interest balancing process.

11.154 Telstra advocated an emergency services exemption.[174] The Australian Bureau of Statistics (ABS) sought an exemption for the use of official data for statistical and related purposes.[175]

11.155 SBS suggested an exemption for journalists and media organisations, provided the serious invasion of privacy occurs while they are engaged in journalism.[176] This would operate in a similar fashion to the journalism exemption in the *Privacy Act*. However, the fault requirement and the public interest balancing process already provide significant protection for the media.

11.156 The Australian Bankers' Association argued that compliance with the *Privacy Act* should be a complete exemption to a statutory cause of action for serious invasion of privacy.[177] This may have been more appropriate if the statutory cause of action could rest on negligence, where whether or not an entity had failed to follow proper practice would be relevant. However, a plaintiff would be unlikely to make out the elements of the tort where an entity's conduct complied with the requirements of the *Privacy Act*.

11.157 The Arts Law Centre of Australia (supported by NAVA and the Australian Institute of Professional Photography) favoured the following exemptions:

---

172 See, eg, *Law Reform (Miscellaneous Provisions) Act 1965* (NSW).

173 Office of the Australian Information Commissioner, *Submission 66*; NSW Young Lawyers, *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*.

174 Telstra, *Submission 45*.

175 Australian Bureau of Statistics, *Submission 32*.

176 SBS, *Submission 59*.

177 Australian Bankers' Association, *Submission 27*.

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.[178] However, the reasonable expectation of privacy, the limited fault element and the public interest balancing test for actionability should provide significant protection for photographers in the range of situations for which exemptions are sought.

11.158 Voiceless and the Barristers' 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'.[179] The ALRC considers that such a defence would be extremely wide, could extensively curtail and infringe civil liberties in a wide range of circumstances and would undermine the protection that the tort is designed to provide from invasive conduct exceeding lawful authority. The balancing test and the defences of lawful authority, necessity and for conduct incidental to the exercise of a lawful right of defence of persons or property, recommended above, more appropriately balance competing interests.

178 Arts Law Centre of Australia, *Submission 43*.
179 Barristers' Animal Welfare Panel and Voiceless, *Submission 64*.

12. Remedies and Costs

Contents

Summary 219
Damages 220
Damages to compensate a plaintiff 221
Factors relevant to the assessment of damages 226
No separate award of aggravated damages 232
Exemplary damages 233
Cap on damages 236
Account of profits 238
No recommendation on notional licence fee 240
Injunctions 241
Injunctions in defamation and breach of confidence 245
Injunctions to restrain disclosure of *private* information 247
Delivery up, destruction or removal of material 251
Correction orders 252
Apology orders 254
Declarations 256
Costs 258

Summary

12.1 This chapter considers the remedies for an action for serious invasion of privacy. The ALRC recommends that courts be empowered to award any one or more of a range of remedies—monetary and non-monetary—to plaintiffs who successfully bring proceedings under the new privacy tort. One benefit of a cause of action being enacted by statute is the capacity and freedom of parliament to provide for a range of remedies, in contrast to the common law which is constrained by precedent and opportunity.

12.2 Serious invasions of privacy may have diverse consequences for plaintiffs. The range of remedies the ALRC recommends in this chapter are appropriate to the different objectives, experiences 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. In some cases, non-monetary remedies may provide a more appropriate response for the often immeasurable effects occasioned by invasions of privacy, or a more effective means to prevent invasions in the future.

12.3 This chapter begins with the ALRC's recommendation that courts be empowered to award damages, including general damages for any emotional distress suffered by the plaintiff. Most actions for invasion of privacy will concern harm to dignitary interests or emotional distress.

12.4 The ALRC recommends that a separate award of aggravated damages should not be made. Rather, the ALRC recommends that a court be empowered to consider a range of factors that may aggravate or mitigate the assessment of damages.

12.5 The ALRC also recommends that a court should have the discretion to award exemplary damages in exceptional circumstances.

12.6 The ALRC recommends a cap on damages. The cap should apply to the sum of both damages for non-economic loss and any exemplary damages. This cap should not exceed the cap on damages for non-economic loss in defamation.

12.7 The ALRC recommends that a court be empowered to award an account of profits in circumstances where a defendant has profited from an invasion of privacy.

12.8 Finally, the ALRC recommends that courts be empowered to award a range of non-monetary remedies where they would be appropriate in the circumstances: 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 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. A non-monetary order such as injunctive or declaratory relief will not necessarily reduce an award of damages.

Damages

Recommendation 12–1 The Act should provide that courts may award damages, including damages for emotional distress.

12.9 The ALRC recommends that damages, including general damages for emotional distress, be available as a remedy for serious invasions of privacy. Previous law reform inquiries made similar recommendations.[1] Several stakeholders supported this recommendation.[2]

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 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Redfern Legal Centre, *Submission 94*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; N Witzleb, *Submission 29*.

12.10 Damages are said to be the 'prime remedy' in tort actions.[3] This is so even where the tort, as the ALRC recommends in the case of the new tort of serious invasion of privacy, is actionable per se in the sense that the plaintiff need not prove any 'actual damage' (personal or psychiatric injury, material damage or financial loss).

12.11 There are four types of damages that may be awarded in a tort action: nominal damages, compensatory damages, aggravated damages and exemplary or punitive damages.

12.12 It is likely that nominal damages will only rarely, if ever, be appropriate where the new tort is made out, because of the requirement of seriousness as an element of the tort. Nominal damages, usually of a token sum,[4] are awarded where a tort is actionable per se and where the plaintiff is unable to prove any injury, loss or damage.[5] It provides mere recognition that the wrong has occurred but where the wrong was not a serious infringement of the plaintiff's rights.

12.13 The most important damages are compensatory damages. How compensatory damages should be assessed in cases of serious invasions of privacy is discussed below.

Damages to compensate a plaintiff

12.14 Compensation is recognised as the dominant purpose of civil actions.[6] The ALRC's recommendation that the statutory cause of action be described as an action in tort[7] will allow a court, when determining damages for a serious invasion of privacy, to draw on principles that have been well settled and applied by the courts in analogous common law actions.

12.15 The purpose of compensatory damages in tort law is to place a plaintiff as far as possible in the position in which they would have been, had the wrong not occurred.[8] It has been argued that this purpose is not commensurate with the nature of a privacy tort as the harm caused by an invasion of privacy is irreversible.[9] However, in most civil actions, where the loss is other than purely financial, damages will not be able to restore a plaintiff to the position they would have been in had the wrong not occurred. Damages cannot undo personal or psychiatric injury. They can however compensate

---

3 *New South Wales v Stevens* (2010) 82 NSWLR 106, [14] (McColl JA). McColl JA was quoting from *Cassell & Co Ltd v Broome* [1971] AC 1027, [1070] (Lord Hailsham).

4 John Mayne and Harvey McGregor, *Mayne & McGregor on Damages* (Sweet & Maxwell, Limited, 12th ed, 1961) [10–006]. See, also, Maule J's statement that 'nominal damages means a sum of money that may be spoken of, but that has no existence in point of quantity': *Beaumont v Greathead* (1846) 2 CB 494, [444].

5 Mayne and McGregor, above n 4, [10–001]. Nominal damages are available in trespass cases: Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [27.3].

6 Robyn Carroll, 'Apologies as a Legal Remedy' (2013) 35 *Sydney Law Review* 317, 340.

7 See Ch 4.

8 *Livingstone v Rawyards Coal Co* (1880) 5 App Cas 25 (Lord Blackburn).

9 Siewert Lindenbergh in Katja Ziegler (ed), *Human Rights and Private Law: Privacy as Autonomy* (Hart Publishing, 2007) 93.

for the financial losses flowing from the injury and provide a measure of solace for the wrong that has occurred.[10]

12.16 Compensatory damages may include special and general damages. 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'.[11] General damages refer to all injuries which are not capable of precise calculation.[12]

Compensation for actual damage

12.17 An award of damages compensates for actual damage to the plaintiff. Actual damage can consist of physical or psychiatric injury, property damage[13] or other economic loss. Plaintiffs must prove that the damage was caused by the tort and fell within the relevant principles of 'remoteness of damage'.[14]

Compensation in the absence of actual damage

12.18 The recommendation that the new tort be actionable *per se* means that a plaintiff need not prove that he or she has suffered personal injury or another form of actual damage in order to bring the action.[15] However, this does not mean that the plaintiff is not entitled to damages for the wrong. As explained in Chapter 8, in a sense the invasion of privacy is both the wrong and the injury, and the plaintiff is entitled to be compensated because it happened.

12.19 The action for invasion of privacy essentially protects a dignitary interest. It is closely analogous to actions like assault and false imprisonment, and other forms of trespass which are actionable per se. The courts deciding actions for invasion of privacy are likely to draw on the principles of damages as developed by the courts in these torts.

12.20 Because the wrong must be serious to be actionable, it is likely that, in the absence of any actual damage, the court will award general damages in order to:

- vindicate the plaintiff;
- compensate the plaintiff for any emotional distress or injury to feelings.

Vindicatory effect of damages awards

12.21 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

---

10 Ibid 98.
11 Balkin and Davis, above n 5, [27.5].
12 Ibid.
13 For example, damage to stock or the cost of repairs to property occasioned by trespass to land or trespass to goods: Ibid [5.15].
14 For an intentional tort, the plaintiff may claim any damage which is a natural and probable consequence of the tort: *Palmer Bruyn & Parker Pty Ltd v Parsons* (2001) 208 CLR 388.
15 See Rec 8–2.

harm to the plaintiff's reputation from a defamatory statement is presumed,[16] an award of general compensatory damages may vindicate a plaintiff's interest.[17]

12.22 While vindication will have a role in compensating people for a serious invasion of privacy, by the acknowledgment that a serious wrong has been a committed, the assessment may be more analogous to other torts protecting privacy—such as trespass to land.

12.23 In *Plenty v Dillon*, Gaudron and McHugh JJ of the High Court of Australia characterised an award of general damages, for what they described as a 'serious' trespass to land, as fulfilling vindicatory purposes:

> True it is that the entry itself caused no damage to the appellant's land. But the purpose of an action for trespass to land is not merely to compensate the plaintiff for damage to the land. That action also serves the purpose of vindicating the plaintiff's right to the exclusive use and occupation of his or her land. The appellant is entitled to have his right of property vindicated by a substantial award of damages ... If the occupier of property has a right not to be unlawfully invaded, then ... the 'right must be supported by an effective sanction otherwise the term will be just meaningless rhetoric'.[18]

12.24 Vindication may be one of multiple aims of compensatory damages in a specific case. However, each aim does not need to be separately compensated.[19] An award of general damages can have several purposes or effects. As the High Court recognised in relation to damages for defamation in *Carson v John Fairfax & Sons Limited & Slee*, 'the amount of a verdict is the product of a mixture of inextricable considerations'.[20]

12.25 A related and unresolved issue is whether a plaintiff may claim harm to reputation in a claim for invasion of privacy. To decide this matter would require a detailed analysis of the new and developing privacy rights and their interaction with defamation. Refusing to strike out such a claim, Mann J in the High Court of England and Wales described this point as 'a serious one, capable of going to the heart of the

---

16 Balkin and Davis, above n 5, [18.17].

17 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.

18 *Plenty v Dillon* (1991) 171 CLR 635, 655.

19 In a recent case of invasion of privacy in the UK, Eady J commented that 'It is accepted in recent jurisprudence that a legitimate consideration is that of vindication to mark the infringement of a right ... If other factors mean that significant damages are to be awarded, in any event, the element of vindication does not need to be reflected in an even higher award': *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB) (Eady J). See, also, Kit Barker, 'The Mixed Concept of Vindication' in Jason Neyers, Erika Chamberlain and Stephen Pitel (eds), *Tort Law: Challenging Orthodoxy* (Hart Publishing, 2013).

20 *Carson v John Fairfax & Sons Limited & Slee* (1993) 178 CLR 44, [60]. See, also**,** *Ell v Milne (No 8)* [2014] NSWSC 175 (7 March 2014) 66. In *Carson v John Fairfax*, the High Court cite *Triggell v Pheeney* (1951) 82 CLR 513. There has been some reference by UK courts when hearing actions for misuse of personal information, to vindicatory damages as a separate head of damages: *Lumba (WL) v Secretary of State for the Home Department* [2012] 1 AC 245 [97]. However, in a 2014 UK case, Dingemans J stated that: 'the effect of an award might be said in general terms to 'vindicate' the Claimant. However the use of the phrase "vindicatory damages" in this area of law is in my judgment unhelpful and liable to mislead, by creating a consequential risk of either overcompensation because of double counting, or under compensation because relevant features about the conduct are not considered': *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB).

cause of action in confidence and the newly developing wrong relating to the invasion of privacy'.[21] He acknowledged that a disclosure might well cause embarrassment and harm to reputation, but the latter would not be actionable where the information was true. He went on:

> It is not clear to me why, as a matter of principle, damage to reputation of this sort should not be within the sort of thing that privacy rights should protect against.[22]

12.26 If this issue arises under the new tort, it will be a matter for the courts to decide.

Damages for emotional or mental distress

12.27 The ALRC recommends that an award of damages under the new tort may, where appropriate, include general damages for emotional distress. This accords with the purpose of a privacy action:

> to promote and protect the physical, psychological and social development of individuals, and their autonomy to decide how they wish to be presented to the world.[23]

12.28 Damages for intangible losses—such as injury to feelings—may provide compensation and solace to a plaintiff.[24] The availability of damages for emotional distress is consistent with the recommendation that only *serious* invasions of privacy would be actionable and that, in determining seriousness, the 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.

12.29 It is highly probable that serious invasions of privacy will commonly cause emotional distress or harm to a plaintiff's dignitary interests.[25] As the High Court of England and Wales recognised in *Mosley*, 'it is reasonable to suppose that damages for such an infringement may include distress, hurt feelings and loss of dignity'.[26]

12.30 This recommendation is consistent with the availability of damages for emotional distress in limited areas of tort law. For instance, damages in trespass cases involving assault, battery and false imprisonment commonly include a component for injury to feelings or mental distress caused by the tort, as do cases of malicious prosecution and defamation.[27]

12.31 The ability to award damages for emotional distress under the new tort will partly fill a significant gap in redress available under existing common law for the

---

21 *Hannon v News Group Newspapers Ltd* [2014] EWHC 1580 (Ch) [27].
22 Ibid [29].
23 John Hartshorne, 'The Value of Privacy' (2010) 2 *Journal of Media Law* 67, 70.
24 Carolyn Sappideen and Prue Vines (eds), *Fleming's The Law of Torts* (Lawbook Co, 10th ed, 2011) [10.110].
25 Public Interest Advocacy Centre, *Submission 105*. See, also, 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, 161.
26 *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB), [216] (Eady J).
27 Tilbury, above n 25, 143.

intentional infliction of emotional distress outside actions such as trespass.[28] As discussed in Chapters 3 and 13, the limitations in the common law are increased by uncertainty about whether compensation for emotional distress is available in equitable actions for breach of confidence.[29]

12.32 Several stakeholders expressed strong support for this recommendation.[30] Redfern Legal Centre argued that

> it is essential that courts also be given the power to award damages for an individual's emotional distress as a result of a serious invasion of privacy. As the ALRC recognises, serious invasions of privacy commonly cause emotional distress or harm to a person's dignitary interests irrespective of whether there was also an economic loss. For our clients, many of who are socio-economically disadvantaged or marginalised, there may be little economic loss arising from a breach of their privacy as they are unemployed and/or have incapacitating disabilities and rely solely on government benefits for support. Nor may they experience an injury that is either physical or amounting to a psychological disorder. It is the emotional damage or loss to their dignity and the hurt and loss of trust caused by the privacy breach that is their greatest concern and one that in our view often necessitates an award of damages to compensate for this loss.[31]

12.33 Dr Normann Witzleb also supported the recommendation, arguing that

> the harm caused by an invasion of privacy will often also be intangible so that any provable loss is likely to be small. An award limited to compensating material loss will therefore often be insufficient to counteract the wrong. Effective redress requires that the plaintiff can also claim compensation for intangible losses, such as injury to feelings.[32]

The likely range of general damages in privacy actions

12.34 The ALRC does not suggest a monetary range for general damages in actions for serious invasion of privacy. Courts will be likely to look at damages awarded in comparable cases for other torts.

12.35 Case law in the UK suggests that the amount of general damages awarded in actions for misuse of personal information for hurt feelings and distress may be 'modest'.[33] Associate Professor Paul Wragg comments:

> What can be achieved by a monetary award in the circumstances is limited. Any award must be proportionate and avoid the appearance of arbitrariness.[34]

---

28 Telstra argued against allowing damages for mental distress on the basis that it is not recoverable in other areas of tort: Telstra, *Submission 107*.

29 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 13 for further discussion.

30 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 97*; Redfern Legal Centre, *Submission 94*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; N Witzleb, *Submission 29*.

31 Redfern Legal Centre, *Submission 94*.

32 N Witzleb, *Submission 29*.

33 *Applause Store Productions Ltd v Raphael* [2008] EWHC 1781 (QB).

12.36 The amount awarded in *Mosley* (£60,000) represents the highest award in a privacy case in the UK to date. In *Weller v Associated Newspapers Ltd,* Dingemans J noted the relatively modest awards in privacy cases:

> Analysis of the cases ... shows that, with the exception of *Mosley*, very substantial awards have not been made in this area. There was an award of £2,500 (and aggravated damages of £1,000) for the publication of the photographs in *Campbell v MGN*; an award of £2,500 for the publication of medical information in *Archer v Williams*; £3,500 for each Claimant for the publication of the photographs in *Douglas v Hello! (No 3)*; and £2,000 for the publication of private information about protected characteristics in *Applause Store Productions Limited v Raphael*.
>
> In *Mosley* the award of damages was for £60,000, and in *AAA* the award of damages was for £15,000 ... for publication on three separate occasions.
>
> It should be noted in *Spelman v Express Newspapers* Tugendhat J recorded that the sums awarded in the early cases for misuse of private information were very low, and that those levels were not the limit of the Court's powers.[35]

12.37 Australian courts may take some guidance from European human rights jurisprudence as to the appropriate award of non-pecuniary damages. Article 41 of the European Convention on Human Rights allows damages to be awarded to the 'just satisfaction' of the injured party.[36] This principle was applied in the case of *Peck v UK*, where the plaintiff was awarded £7,500 for non-pecuniary loss owing to the 'distress, anxiety, embarrassment and frustration' suffered as a consequence of CCTV footage of him attempting to commit suicide being broadcast on national television.[37]

12.38 Wragg suggests that the qualitative difference between the two types of privacy invasions in the new tort—intrusion upon seclusion and misuse of private information—may mean that the damages awarded in different cases are assessed differently.[38]

12.39 In other jurisdictions, courts have developed different approaches to assessing damages. In *Jones v Tsige,* Sharpe JA assessed damages based on a number of factors in that case, including whether the plaintiff suffered 'public embarrassment or harm to her health, welfare, social, business or financial position'.[39] He suggested that damages for intrusion should be modest.[40]

Factors relevant to the assessment of damages

Recommendation 12–2 The Act should set out the following non-exhaustive list of factors that a court may consider when determining the amount of damages:

34 P Wragg, *Submission 73*.
35 *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB), [193]–[195].
36 *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).
37 *Peck v United Kingdom* [2003] ECHR 44 (28 January 2003) [117].
38 P Wragg, *Submission 73*.
39 *Jones v Tsige* (2012) ONCA 32, [90].
40 Ibid [87].

(a) whether the defendant had made an appropriate apology to the plaintiff;

(b) whether the defendant had published a correction;

(c) whether the plaintiff had already recovered compensation, or has agreed to receive compensation in relation to the conduct of the defendant;

(d) whether either party took reasonable steps to settle the dispute without litigation; and

(e) whether the defendant's unreasonable conduct following the invasion of privacy, including during the proceedings, had subjected the plaintiff to particular or additional embarrassment, harm, distress or humiliation.

12.40 The ALRC recommends that in assessing damages in an action for serious invasion of privacy, a court may consider a number of factors as mitigating or aggravating general damages.

12.41 These factors are designed to encourage parties to resolve a matter before litigation or before litigation proceeds to a hearing. This is a non-exhaustive list. It is intended to guide a court when determining the assessment of damages. It will be for the court to decide whether particular factors are relevant.

12.42 Mitigating factors will have the effect of reducing the harm of a 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. The consideration of a defendant's conduct up to and including conduct at trial is relevant in the assessment of damages in other intentional torts, particularly for false imprisonment[41] and defamation.[42]

12.43 The Uniform Defamation Law contains similar factors for a court to consider in the award of damages. For instance, s 38 of the *Defamation Act 2005* (NSW) sets out mitigating factors for a court to consider when assessing damages, including whether the defendant has made an apology to the plaintiff or has published a correction of the defamatory matter.

12.44 In actions for misuse of personal information in the UK, courts have considered the effect of mitigating or aggravating conduct or circumstances in the award of damages. While there was no separate award of aggravated damages in *Mosley* for instance, aggravating conduct was relevant to the assessment of the award of general damages. Eady J commented:

> It must be recognised that it may be appropriate to take into account any aggravating conduct in privacy cases on the part of the defendant which increases

41 *Spautz v Butterworth* (1996) 41 NSWLR 1.
42 Mayne and McGregor, above n 4, [7–009].

> the hurt to the claimant's feelings or 'rubs salt in the wound'. As Lord Reid said, in the context of defamation, in *Cassell v Broome*:
>
> 'It has long been recognised that in determining what sum within that bracket should be awarded, a jury, or other tribunal, is entitled to have regard to the conduct of the defendant. He may have behaved in a highhanded, malicious, insulting or oppressive manner in committing the tort or he or his counsel may at the trial have aggravated the injury by what they there said. That would justify going to the top of the bracket and awarding as damages the largest sum that could fairly be regarded as compensation'.[43]

12.45 Several stakeholders supported this list of factors.[44] Telstra underscored their particular support for factors (a) and (d).[45] Detail about some of the factors is provided below.

(a) and (b) whether the defendant issued an apology or correction

12.46 Where a defendant has made an apology or issued a clear correction of false information about an individual, a court may consider these as mitigating factors in an award of damages. These two factors will be particularly relevant to invasions that occur through the publication of an individual's private information.

12.47 Defamation law includes apologies or corrections as mitigating factors in the assessment of damages.[46] Apologies are not a remedy at common law for intentional torts, instead they are often a factor mitigating an award of damages.[47] The Canadian *Privacy Acts* also include apologies as a mitigating factor in the assessment of damages.[48]

12.48 Several stakeholders argued that this practice should be encouraged to promote the resolution of matters prior to or during litigation.[49] Guardian News and Media Limited and Guardian Australia argued that 'the nature of invasions of privacy is that in many instances an apology, freely given, may be sufficient to resolve the matter.[50]

12.49 Research into the role of apologies on the settlement decision-making processes of litigants in America suggests that apologies influence claimants' perceptions, judgments and decisions in ways that make settlement more likely.[51] Resolving privacy

---

43 *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB), [222] (Eady J). Eady J cited *Cassell & Co Ltd v Broome* [1971] AC 1027, 1085. In *Mosley*, Eady J also considered that damages may be mitigated by reference to the conduct of a plaintiff. In obiter, he questioned to what extent a plaintiff's conduct prior to the invasion of their privacy could be considered in the assessment of damages, if their conduct contributed to their distress: *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB), [224]–[226].

44 T Butler, *Submission 114*; Arts Law Centre of Australia, *Submission 113*; Telstra, *Submission 107*; Australian Sex Party, *Submission 92*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

45 Telstra, *Submission 45*.

46 See, eg, *Defamation Act 2005* (NSW) 2005 s 38(1)(a)–(b).

47 See, eg, Ibid s 38(1)(a).

48 See, eg, *Privacy Act*, CCSM 1996, c P125 (Manitoba) s 4(2)(e).

49 Guardian News and Media Limited and Guardian Australia, *Submission 80*; Telecommunications Industry Ombudsman, *Submission 103*.

50 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

51 Carroll, above n 6, 319.

disputes prior to the commencement of costly legal proceedings will, generally speaking, be advantageous to both parties.

12.50 The Insurance Council of Australia argued that an apology or correction should not be included as a factor to mitigate damages as these remedies are inconsistent with the aim of protecting a person's privacy.[52] The issuing of a public correction or apology for publication of false private information may compound the emotional distress, hurt or embarrassment occasioned by the initial invasion of privacy.

12.51 Some stakeholders argued that the term 'apology' should be qualified to ensure they are given in a genuine or sincere fashion.[53] The ALRC considers that a court will necessarily take the relevant circumstances into account when assessing the nature and effectiveness of any apology or correction made prior to the commencement of legal proceedings.

(c) whether the plaintiff has already recovered compensation, or has agreed to receive compensation in relation to the conduct of the defendant

12.52 This factor recognises that it would be unfair for a plaintiff to be compensated more than once in relation to the same invasion of privacy. Where a plaintiff has pursued alternative dispute resolution (ADR) or some other complaints mechanism prior to undertaking legal proceedings under the new privacy tort, a court should consider any compensation or other remedy obtained when assessing damages.

12.53 There are several legal or regulatory avenues that a plaintiff may be able to pursue as an alternative to taking action under the new privacy tort. These may result in the payment of compensation or an award of damages. For example, the Office of the Australian Information Commissioner (OAIC) has the power to make determinations that an APP entity must provide compensation to an individual where it is found that APP entity breached an Australian Privacy Principle.[54] In Chapter 16, the ALRC supports the OAIC's proposal to broaden the complaints mechanism. In Queensland, the *Information Privacy Act* empowers the Privacy Commissioner to refer complaints to the Queensland Civil and Administrative Tribunal (QCAT).[55]

12.54 Were a plaintiff to pursue either of these avenues prior to commencing legal proceedings under the new privacy tort, a court should take into account any compensation already awarded, agreed upon, or received, when assessing damages.

12.55 However, the ALRC does not recommend a bar on legal proceedings under the new privacy tort where a plaintiff has already pursued the matter through another mechanism.

---

52 Insurance Council of Australia, *Submission 102*.

53 S Higgins, *Submission 82*; I Turnbull, *Submission 81*.

54 *Privacy Act 1988* (Cth) s 42.

55 QCAT can hear those complaints in its original jurisdiction and may make an order for compensation of up to $100, 000: *Information Privacy Act 2009* (Qld) s 176(1)–(2).

(d) whether either party took reasonable steps to settle a dispute

12.56 This factor is intended to encourage the parties, in appropriate circumstances, to attempt to resolve their dispute without litigation, if it would be reasonable to expect them to do so.[56] This factor may be read as a mitigating or an aggravating factor in the assessment of an award of damages, depending on whether a party took 'reasonable steps' to settle a dispute prior to legal proceedings.

12.57 In determining the 'reasonableness' of either party's conduct, a court may consider whether either party had made attempts at ADR; whether a complaint had first been made to the Office of the Australian Information Commissioner, the Australian Communications and Media Authority (the ACMA) or another body, and the outcome of any determination.

12.58 Whether a defendant has made an offer of amends—and whether that offer has been accepted—may be considered by a court when assessing whether either party has taken reasonable steps to settle a dispute prior to legal proceedings.

12.59 When determining reasonableness, a court may consider whether the nature of the invasion of privacy—particularly where it is ongoing—as well as the relationship between the parties, is conducive to pre-litigation resolution.

12.60 Given the highly personal nature of some invasions of privacy, there may be many circumstances where pre-trial negotiations are inappropriate. Advocates for persons experiencing domestic violence were concerned by the inclusion of this factor in the list of mitigating and aggravating factors.[57] The Office of the Victorian Privacy Commissioner argued that ADR can sometimes lead to inequitable outcomes for some plaintiffs, particularly in situations where there is a perceived power imbalance between two parties to a proceeding; a lack of trust between the parties; or where the plaintiff may be too emotionally distressed to approach the plaintiff.[58]

12.61 The ALRC agrees that the circumstances of some invasions of privacy will be inappropriate for pre-trial ADR. The ALRC also agrees that failure by a plaintiff to engage with a defendant who shows a willingness to settle a dispute prior to legal proceedings should only be used against a plaintiff in an award of damages, where it would be reasonable to do so in the circumstances.

12.62 The ALRC has not proposed that ADR be compulsory before pursuing an action for serious invasion of privacy, but instead considers that including this factor will encourage parties to engage in ADR where appropriate.

---

56 This is consistent with the policy intent behind the *Civil Dispute Resolution Act 2011* (Cth). Its objects clause encourages 'as far as possible, people taking genuine steps to resolve disputes before certain civil proceedings are instituted': Ibid s 3.

57 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Office of the Victorian Privacy Commissioner, *Submission 108*; N Henry and A Powell, *Submission 104*.

58 Office of the Victorian Privacy Commissioner, *Submission 108*.

Contributory negligence should not be considered in assessing damages

12.63 The ALRC recommends that contributory negligence not 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,[59] 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.[60] As discussed in Chapter 11, contributory negligence is not recommended as a defence to the new tort.

12.64 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. However, as Eady J pointed out in *Mosley,*

> there is no doctrine of contributory negligence. On the other hand, the extent to which his own conduct has contributed to the nature and scale of the distress might be a relevant factor on causation. Has he, for example, put himself in a predicament by his own choice which contributed to his distress and loss of dignity?[61]

Other factors

12.65 The ALRC has not recommended that the defendant's state of mind at the time of the invasion of the privacy should be considered. However, it will be a matter for the court whether this should be considered in a particular case. In some circumstances, a high level of malice may be more appropriately considered as grounds for an award of exemplary damages, because exemplary damages focus on the defendant's motives.[62]

12.66 Several stakeholders proposed additional factors in mitigation or aggravation of damages. The ABC proposed that 'whether the defendant reasonably believed that the actions comprising the invasion were carried out in the public interest' should be considered.[63] However, the ALRC considers the public interest balancing test is already a sufficient protection of legitimate and reasonable claims for public interest disclosure of an individual's private information.

12.67 The Australian Bankers' Association (ABA) proposed that if the defendant acted 'honestly and reasonably', they 'ought fairly to be excused'.[64] This is similar to a provision in the Australian Consumer Law (ACL) which provides a defence where a person 'acted honestly and reasonably and, having regard to all the circumstances of the case, ought fairly to be excused, the Court may relieve the person either wholly or partly from liability to any penalty or damages on such terms as the Court thinks fit'.[65]

---

59 See, eg, *Law Reform (Miscellaneous Provisions) Act 1965* (NSW) s 9.
60 *Horkin v North Melbourne Football Club* (1983) 1 VR 153.
61 *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB), [244].
62 Mayne and McGregor, above n 4, [11–009].
63 ABC, *Submission 93*.
64 Australian Bankers' Association, *Submission 84*.
65 *Competition and Consumer Act 2010* (Cth) s 85.

However, the fault element of the new tort makes such relief from liability to pay damages less appropriate than in the case of the ACL which imposes strict liability.

No separate award of aggravated damages

Recommendation 12–3 The Act should provide that the court may not award a separate sum as aggravated damages.

12.68 The ALRC recommends that the Act should not empower a court to make a separate award for aggravated damages.[66]

12.69 At common law, aggravated damages are a form of general damages, 'given by way of compensation for injury to the plaintiff, which may be intangible, resulting from the circumstances and manner of the wrongdoing'.[67]

12.70 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.[68] Aggravated damages are awarded where the defendant's conduct was so outrageous that an increased award is necessary to appropriately compensate injury to a plaintiff's 'proper feelings of dignity and pride'.[69]

12.71 Rather than recommending that aggravated damages may be awarded, the ALRC recommends that a court may consider whether a defendant's unreasonable conduct following the invasion of privacy, or prior to or during legal proceedings, subjected the plaintiff to special or additional embarrassment, harm, distress or humiliation when assessing damages.[70]

12.72 The ALRC considers that listing such conduct as a factor to be considered when assessing damages will provide sufficient opportunity for the court to take into account circumstances where a defendant has caused additional and unreasonable distress or humiliation to a plaintiff prior to commencing legal proceedings.[71] Moreover, the ALRC recommends that exemplary damages may be awarded where a court believes it is appropriate in all the circumstances.

12.73 The ALRC recommends that aggravated damages not be awarded as a separate sum to avoid the risk of overlap between an ordinary award of general damages for injury to the plaintiff's feelings and an award of aggravated damages.[72]

---

66 Several stakeholders supported this recommendation: Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*.

67 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 129–130 (Taylor J).

68 '[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).

69 *Rookes v Barnard* [1964] AC 1129 [1221] (Lord Devlin).

70 Rec 12–2(e).

71 The Australian Sex Party agreed with this point: Australian Sex Party, *Submission 92*.

72 *New South Wales v Riley* (2003) 57 NSWLR 496, [129]. This passage was quoted by Sackville AJA in *New South Wales v Radford* (2010) 79 NSWLR 327, [96].

12.74 There is also a risk of overlap between the award for aggravated damages and that for exemplary damages, considered later in this chapter, which are intended to punish or deter the defendant because of the nature of his or her 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'.[73] Both risks are avoided if aggravated damages cannot be awarded.

12.75 The ALRC's approach is consistent with that of the New South Wales Law Reform Commission (NSWLRC) on this issue. The NSWLRC explained that aggravating circumstances would already form some part of an assessment for general damages, stating:

> 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.[74]

Exemplary damages

Recommendation 12–4 The Act should provide that a court may award exemplary damages in exceptional circumstances.

12.76 The ALRC recommends that a court be given the discretion to award exemplary damages in exceptional circumstances, where a defendant's conduct was outrageous and in contumelious disregard of a plaintiff's rights.[75] An award for exemplary damages is considered separately from other heads of damages.[76] Exemplary damages are intended to punish a defendant and deter similar conduct in the future.

12.77 The ALRC considers that the award of exemplary damages should only be made in exceptional circumstances or, for example, where the court considers that the other damages or remedy awarded would not provide a sufficient deterrent against similar conduct in the future. The deterrent function of exemplary damages is arguably more valuable than the punitive function. The aim of awarding exemplary damages to deter similar conduct by others in the future has been recognised by Australian courts.[77]

12.78 When assessing whether the exceptional circumstances of the case call for an award of exemplary damages, the court will also consider whether the other damages

---

73 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 129–130 (Taylor J).

74 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [7.10].

75 Several stakeholders supported the availability of an award of exemplary damages in exceptional circumstances: Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; P Wragg, *Submission 73*; Australian Privacy Foundation, *Submission 39*; N Witzleb, *Submission 29*; Law Institute of Victoria, *Submission 22*; Women's Legal Centre (ACT & Region) Inc, *Submission 19*; T Gardner, *Submission 3*.

76 *Henry v Thompson* (1989) 2 Qd R 412.

77 *Lamb v Cotogno* (1987) 164 CLR 1, [13].

already awarded against the defendant are sufficient to fulfil the retributive, punitive or deterrent purposes of exemplary damages.[78]

12.79 The ALRC considers that a court should be able to award exemplary damages under the new privacy tort, given that it is confined to invasions of privacy that are both serious and intentional or reckless.[79] The ALRC intends that any award of exemplary damages should be included in the cap on damages for non-economic loss, as outlined in Recommendation 12–5 later in this chapter.

12.80 Exemplary damages are available in Australia at common law for a wide range of intentional torts.[80] They are not available in defamation claims.[81] They are also not available for breach of equitable obligations such as breach of confidence,[82] or in actions for breach of a contractual duty of confidence,[83] and are limited in personal injury actions.[84]

12.81 Exemplary damages are available in privacy actions in other jurisdictions. In the UK, the 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.[85]

12.82 Similarly, the Joint Committee of the House of Lords and House of Commons on Privacy and Injunctions recommended in 2012 that courts be empowered to award exemplary damages in privacy cases, arguing that compensatory damages were too low to act as an effective deterrent.[86] 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.[87] Under this provision, a court may only award exemplary damages where the defendant's conduct has shown a deliberate or reckless disregard of an outrageous nature for the

78 *New South Wales v Ibbett* (2006) 229 CLR 638, [34].

79 See Chs 7 and 8. The ALRC notes that there is some divergence of opinion whether exemplary damages should be available for a civil action: see Balkin and Davis, above n 5, [11–001].

80 *Lamb v Cotogno* (1987) 164 CLR 1; Balkin and Davis, above n 5, [11–001]. 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.

81 See, eg, *Defamation Act 2005* (NSW) 2005 s 35.

82 *Giller v Procopets* (2008) 24 VR 1. In that case, 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* [2008] EWHC 1777 (QB), [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. In that case, the court overturned an award of exemplary damages for breach of fiduciary duty.

83 This is in contrast to the UK approach: *Attorney General v Blake* [2001] 1 AC 268.

84 See, eg, *Civil Liability Act 2002* (NSW) s 21. This provision abolishes exemptions for negligently inflicting personal injury.

85 Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, House of Commons Paper 779 (2012) vol 4, [5.12].

86 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.

87 *Crime and Courts Act 2013* (UK) s 34. The Guardian News noted that this provision has been the subject of some criticism in the UK: Guardian News and Media Limited and Guardian Australia, *Submission 80*.

claimant's rights;[88] or the conduct is such that the court should punish the defendant for it;[89] and other remedies would not be adequate to punish that conduct.[90] Canadian privacy statutes also provide that courts may award punitive damages.[91]

12.83 PIAC supported the recommendation to allow the award of exemplary damages, arguing that

> there are a number of circumstances where an invasion of privacy may be of such a malicious or high-handed manner that it warrants an award of exemplary damages. PIAC also supports the award of exemplary damages where other damages awarded would be an insufficient deterrent.[92]

12.84 Posting on the internet of 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 that may justify an award of exemplary damages.

12.85 An award of exemplary damages may also be 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.[93]

12.86 Women's legal services generally welcomed the availability of an award of exemplary damages,[94] with Women's Legal Services NSW arguing that

> using exemplary damages in the context of violence against women would send a powerful message that violence against women is unacceptable in our society.[95]

12.87 There is some concern that exemplary damages provide a windfall to plaintiffs.[96] Courts, however, are conscious of this concern and the High Court has ruled that awards of exemplary damages should be moderate.[97]

12.88 Several stakeholders opposed the availability of an award of exemplary damages.[98] The OAIC submitted that remedies for a privacy action should be directed

---

88 *Crime and Courts Act 2013* (UK) s 34(6)(a).
89 Ibid s 34(6)(b).
90 Ibid s 34(6)(c).
91 See, eg, *Privacy Act*, RSBC 1996, c 373 (British Columbia).
92 Public Interest Advocacy Centre, *Submission 105*.
93 N Witzleb, *Submission 29*. Witzleb noted that another value of an award of exemplary damages may be that it will be a means of stripping a defendant of any profit made from an invasion of privacy.
94 Women's Legal Centre (ACT & Region) Inc, *Submission 19*; Women's Legal Services NSW, *Submission 115*.
95 Women's Legal Services NSW, *Submission 115*.
96 Insurance Council of Australia, *Submission 102*.
97 *Xl Petroleum (NSW) Pty Ltd v Caltex Oil (Australia) Pty Ltd* [1985] HCA 12 (28 February 1985).
98 Insurance Council of Australia, *Submission 102*; ABC, *Submission 93*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; SBS, *Submission 59*; Telstra, *Submission 45*; Arts Law Centre of Australia, *Submission 43*.

at compensating a plaintiff, while exemplary damages are targeted at punishing a defendant.[99]

12.89 There is 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.[100] Guardian News argued that the legal costs associated with defending analogous civil actions, such as defamation suits, act as a sufficient deterrent for media organisations to avoid publishing defamatory matter.[101] They argue that this principle would apply to actions brought under the new privacy tort.

12.90 While the ALRC acknowledges the concern that potential defendants would have about the availability of exemplary damages, it considers that the courts should be able to award them in exceptional circumstances.

Cap on damages

Recommendation 12–5 The Act should provide for a cap on damages. The cap should apply to the sum of both damages for non-economic loss and any exemplary damages. This cap should not exceed the cap on damages for non-economic loss in defamation.

12.91 The ALRC recommends a cap on damages for all damages other than for economic loss. Any award for exemplary damages should be included in the amount of damages subject to this cap. The total amount of general damages for non-economic loss and exemplary damages awarded should be capped at the same amount as the cap on damages for non-economic loss in defamation awards.[102]

12.92 This recommendation provides equal protection to privacy and reputational interests and may avoid the risk of plaintiffs cherry-picking between causes of action based on the availability of higher awards of damages.[103]

12.93 Several stakeholders agreed with this recommendation.[104] PIAC opposed the imposition of a cap on damages for non-economic loss, fearing that 'if the ceiling is set too low, it will be inadequate to redress unlawful conduct'. However, if a cap were to be introduced, they supported an alignment with defamation law.[105] Similarly, Barker

---

99 Office of the Australian Information Commissioner, *Submission 66*. Other stakeholders supported this statement: Insurance Council of Australia, *Submission 102*; ABC, *Submission 93*.

100 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

101 Ibid.

102 See, eg, *Defamation Act 2005* (NSW) 2005 s 35. Damages for non-economic loss in defamation were initially capped at $250,000 and, at the time of writing, are $355,000.

103 Nicholas Petrie, 'Reforming the Remedy: Getting the Right Remedial Structure to Protect Personal Privacy' (2012) 17 *Deakin Law Review* 139.

104 T Butler, *Submission 114*; Telstra, *Submission 107*; Redfern Legal Centre, *Submission 94*; ABC, *Submission 93*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

105 Public Interest Advocacy Centre, *Submission 105*.

argued that, while he was unconvinced by the need for a cap on damages, any cap should be set at the same level as defamation:

> since such caps now apply in personal injury and defamation claims in Australia, it would be anomalous and unfair from a distributive point of view if similar caps did not apply. A cap similar to that applied in defamation cases for non-economic loss would seem appropriate.[106]

12.94 Associate Professor David Rolph has argued that a cap on damages for a statutory cause of action should not be lower than that for defamation.[107] He argued that a lower cap on damages for non-economic loss in privacy actions would be 'undesirable, failing to reflect the relative importance Australia should now prescribe to privacy'.[108]

12.95 The ABC supported a cap on damages for non-economic loss, arguing however that the cap should be lower than that in defamation law.[109] The ALRC considers that, while the cap on damages for non-economic loss in defamation is arguably too high, it is nevertheless desirable that the caps be the same for both actions.

12.96 The Redfern Legal Centre supported the proposal, arguing that other statutory privacy schemes provide 'inadequate compensation'.[110] For instance, under the *Health Records and Information Privacy Act 2002* (NSW), the NSW Civil and Administrative Tribunal (NCAT) can award a maximum of $40,000 where the respondent is a body corporate and $10,000 where the case involves any other party.[111] According to Redfern Legal Centre, the maximum amount 'is rarely (if ever) awarded, meaning that a victim is insufficiently compensated for serious breaches of their privacy under this regime'.[112]

12.97 Some stakeholders argued against capping damages.[113] 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'.[114]

12.98 The Office of the Victorian Privacy Commissioner argued that not imposing a cap on damages would 'reflect the growing importance placed on privacy rights in Australia'.[115]

12.99 The ALRC is of the view that an appropriate cap will not undervalue privacy interests, in the same way that a cap on damages for non-economic loss in defamation has not eroded the protection of reputational interests in Australia.

---

106 K Barker, *Submission 126*.
107 David Rolph, 'The Interaction of Remedies for Defamation and Privacy' [2012] *Precedent* 14, 3.
108 Ibid 107.
109 ABC, *Submission 93*.
110 Redfern Legal Centre, *Submission 94*.
111 *Health Records and Information Privacy Act 2002* (NSW) s 54(1)(a).
112 Redfern Legal Centre, *Submission 94*.
113 Office of the Victorian Privacy Commissioner, *Submission 108*; Office of the Australian Information Commissioner, *Submission 66*; Public Interest Advocacy Centre, *Submission 30*.
114 Office of the Australian Information Commissioner, *Submission 66*.
115 Office of the Victorian Privacy Commissioner, *Submission 108*.

12.100 Moreover, the ALRC does not consider that a cap—combined with the threshold requirement that actions be sufficiently 'serious'—poses a risk that courts will automatically award the upper limit in every case. Courts are equipped to assess appropriate awards of damages based on the context in which each case arises. For example, in *Jones v Tsige,* Sharpe JA stated that

> in determining damages, there are a number of factors to consider. Favouring a higher award is the fact that Tsige's actions were deliberate and repeated and arose from a complex web of domestic arrangements likely to provoke strong feelings and animosity. Jones was understandably very upset by the intrusion into her private financial affairs. On the other hand, Jones suffered no public embarrassment or harm to her health, welfare, social, business or financial position and Tsige has apologized for her conduct and made genuine attempts to make amends. On balance, I would place this case at the mid-point of the range I have identified and award damages in the amount of $10,000. Tsige's intrusion upon Jones' seclusion, this case does not, in my view, exhibit any exceptional quality calling for an award of aggravated or punitive damages.[116]

12.101 While the ALRC recommends that a cap be included, it has not recommended a threshold for damages. It will be for the court to decide the appropriate awards in an individual case, taking into account awards for analogous torts.

Account of profits

Recommendation 12–6 The Act should provide that a court may award an account of profits.

12.102 The ALRC recommends that a court be empowered to award an account of profits as a remedy for the new tort.[117] This award would be an alternative to damages. The gains-based remedy of an account of profit has the aim of deterring 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.[118]

12.103 An award of an account of profits may be appropriate where the financial benefit derived to a defendant from an invasion of privacy exceeds the loss incurred to a plaintiff.[119] This remedy may also provide redress to plaintiffs where compensatory damages would be difficult to calculate.

12.104 The availability of an account of profits may also have a deterrent effect on the behaviour of potential defendants when they are considering the commercial benefit to be gained from publishing an individual's private information. It is distinct

---

116 *Jones v Tsige* (2012) ONCA 32, [90] (Sharpe JA).

117 Several stakeholders were in favour of this proposal: N Witzleb, *Submission 116*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Office of the Australian Information Commissioner, *Submission 66*; Public Interest Advocacy Centre, *Submission 30*; Insurance Council of Australia, *Submission 15*; I Turnbull, *Submission 5*.

118 N Witzleb, *Submission 29*.

119 Mayne and McGregor, above n 4, [12–005].

from an award of damages in that it responds to the gain of the wrongdoer rather than the loss of the wronged party.[120] To that end, PIAC argued that

> Orders of this nature will prevent unjust enrichment of respondents and will also act as a deterrent in the case of 'serial respondents', or respondents who are unlikely to be particularly adversely affected by being ordered to pay compensatory damages.[121]

12.105 Similarly, Witzleb argued that 'commercially motivated defendants can only be effectively prevented from invading people's privacy where profit-stripping remedies are made available'.[122]

12.106 An account of profits is an established remedy in actions for breach of confidence.[123] It is also available in some limited types of tort actions, such as passing off.[124]

12.107 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. 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.[125]

12.108 It may be difficult for a plaintiff to prove that the defendant has made a profit or gain from the invasion of privacy. Calculating the profit to be attributed to the publication of private information may be complex where it forms only part of a larger publication. In these cases, a court will determine the reasonableness of the connection between the invasion of privacy and the profit obtained.[126]

12.109 An account of profits was recommended as a remedy for a serious invasion of privacy in ALRC Report 108.[127] The NSWLRC also recommended an account of profits, at least in exceptional cases.[128] Both 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 considered that this should preclude an account of profits being available, if appropriate.

---

120 *Warman International Ltd v Dwyer* (1995) 182 CLR 544.
121 Public Interest Advocacy Centre, *Submission 105*.
122 N Witzleb, *Submission 29*.
123 *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109.
124 Roderick Pitt Meagher, Dyson Heydon and Mark Leeming, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 4th ed, 2002) [25–002].
125 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 497.
126 *CMS Dolphin Ltd v Simonet* [2001] 2 BCLC 704, [97].
127 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5.
128 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [7.23]–[7.24].

12.110 ASTRA argued that an account of profits is a very narrow and particular remedy, which is

> likely to be more effective against a large, established company than against a fledgling web-based media outlet which is more concerned with generating 'likes' or 'followers' than generating profit.[129]

12.111 Some stakeholders argued that an account of profits is an inappropriate remedy for a privacy action as it attaches commercial value to a dignitary interest.[130] However the ALRC considers that, unlike other remedies—such as the calculation of damages based on a notional licence fee—an account of profits is designed to strip a defendant of the benefit of an invasion of privacy rather than to vindicate any commercial interest a plaintiff may wish to pursue.

No recommendation on notional licence fee

12.112 In the Discussion Paper, the ALRC proposed the availability of damages based on the calculation of a notional licence fee. After further consideration and discussion with relevant stakeholders, the ALRC has decided not to make a recommendation that a court may award damages based on a notional licence fee. The ALRC considers that an assessment of damages based on a notional licence fee is primarily aimed at protecting commercial rights rather than personal, dignitary interests such as privacy. As a result, it makes no recommendation that it be available as a remedy for the new tort. Nonetheless, the ALRC considers that it would be a matter for the courts to decide whether this remedy is appropriate in any particular case.

12.113 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. This remedy seeks to target the value to the defendant of deliberately invading the plaintiff's privacy.

12.114 Damages assessed on the basis of notional licence fees have been considered by courts in the UK in actions for breach of confidence and breach of contract. In *Irvine v Talksport*,[131] 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 Court of Appeal of England and Wales recognised that an award based on a notional licence fee was available in situations where a plaintiff had permitted the invasive act in question (in this case, publication of wedding photographs) but had not been compensated for it.[132]

---

129 ASTRA, *Submission 99*.

130 Telstra, *Submission 107*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

131 *Irvine v Talksport Ltd* (2003) 2 ER 881.

132 Sirko Harder, 'Gain-Based Relief for Invasion of Privacy' (2011) 1 *DICTUM—Victoria Law School Journal* 63, 68.

12.115 There is debate about the applicability of gains-based relief for an invasion of privacy. Dr Sirko Harder has 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.[133]

12.116 ASTRA submitted that this remedy was not appropriate for an invasion of privacy, arguing that,

> if an individual is willing to grant a licence for an invasion of privacy (especially when subject to payment of a fee), this should not be actionable under the proposed tort.[134]

12.117 Australian law does not recognise a right of publicity. However, the misappropriation and unauthorised commercial use of an individual's image is protected by the tort of passing off, where that individual has a trading reputation,[135] and other aspects of intellectual property law. The tort of passing off aims to prevent economic loss by redressing misrepresentation which occurs when one party 'passes off' their goods or services as the goods or services of another party.[136] Remedying the commercial consequences of unauthorised publication of private information may be better pursued through the development of the tort of passing off, if available, than through a notional licence fee.

Injunctions

Recommendation 12–7 The Act should provide that the court may at any stage of proceedings grant an interlocutory or other injunction to restrain the threatened or apprehended invasion of privacy, where it appears to the court to be just or convenient and on such terms as the court thinks fit.

Recommendation 12–8 The Act should provide that, when considering whether to grant injunctive relief before trial to restrain publication of private information, a court must have particular regard to freedom of expression and any other matters of public interest.

12.118 In privacy actions, plaintiffs are highly likely to seek a court order or injunction to prevent the commission or continuance of a serious invasion of privacy. For example, a plaintiff may seek to prevent the disclosure or publication of their private information to or by another person or a media entity.

---

133 Ibid 79.
134 ASTRA, *Submission 99*.
135 Normann Witzleb, 'Justifying Gain-Based Remedies for Invasions of Privacy' (2009) 29 *Oxford Journal of Legal Studies* 325, 339.
136 Mayne and McGregor, above n 4, [40–020].

12.119 The power of the courts to order injunctions is usually set out in the enabling statute for the court,[137] and is subject to a substantial body of equitable principles or specific statutory provisions.[138] 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.[139] The court will not grant an injunction where it would be futile to do so: one ground for futility may be the wide publicity already given to the relevant information. Previous law reform inquiries recommended that courts be able to order injunctive relief in relation to the new cause of action.[140]

12.120 In some cases, a final and permanent injunction may be sought at the trial of the action. However, in most privacy cases, the most significant remedy will be an interlocutory injunction to prevent a *threatened* invasion of privacy—such as the broadcast or publication of private information. An interlocutory injunction is sought prior to the trial, sometimes ex parte in cases of great urgency, to maintain the status quo. In the case of a privacy action against the media for example, the status quo would usually be the non-publication of the material.

12.121 In a privacy case, perhaps even more so than in other cases such as defamation cases,[141] the stakes are high for both parties at the interlocutory stage. For the plaintiff, privacy in information, once lost, may be lost forever,[142] and no amount of compensation will render the information entirely private again.[143] For the defendant,

---

137 See, eg, *Supreme Court Act 1970* (NSW) s 66. The provision would apply to both apprehended and continuing invasions of privacy.

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

139 *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.

140 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(c).

141 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.

142 *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.

143 It is difficult to imagine a situation where damages would be an adequate remedy in a case involving a serious invasion of privacy. In trespass cases, the court have sometimes held that damages would be an adequate remedy, and thus, on the threshold equitable test, refused 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 his ground, obviating the need to consider public interest. The view, however, is taken in many cases of serious invasion of privacy

on the other hand, there is the consideration that by the time the entitlement to publish is adjudicated in a final hearing, the appropriate opportunity to reveal the relevant information or to contribute to a public debate may be lost as the information's novelty, relevance or interest is overtaken by other events. As Lord Nicholls noted in *Reynolds v Times Newspapers*: 'News is a perishable commodity'.[144]

12.122 This means that, of all remedies, an interlocutory injunction restraining publication is arguably the most significant restriction on freedom of speech and the freedom of the media to report on matters of public interest and concern. There is therefore a strong and justifiable concern that unmeritorious claims to prevent the disclosure of allegedly 'private' information, in which there is a legitimate public interest, might chill freedom of speech and the freedom of the press.

12.123 The Terms of Reference for this Inquiry require the ALRC to make recommendations as to 'the necessity of balancing privacy with other fundamental values including freedom of expression and open justice'. The most significant recommendation reflecting this necessity is the requirement that the court must be satisfied that, for the plaintiff to have a cause of action, the public interest in privacy outweighs any countervailing public interest.[145]

12.124 In addition, the ALRC recommends that courts should be specifically directed by the legislation to consider freedom of expression and other matters of public interest when considering whether to grant an interlocutory injunction to restrain the publication of private information. This recommendation is based on s 12(4) of the *Human Rights Act 1998* (UK), discussed below.

12.125 In view of the ordinary principles governing the grant of an interlocutory injunction, discussed below, and the requirement for actionability set out in Chapter 8, it may be argued that an additional provision directing courts to consider any matters of public interest when considering an injunction application is unnecessary.

12.126 According to equitable principles, as set out by the High Court of Australia in *Beecham Group v Bristol Laboratories Pty Ltd*[146] and reaffirmed in *ABC v O'Neill*,[147] before the court will exercise its discretion to award an interlocutory injunction, an applicant must satisfy the court that:

---

against individuals that 'no amount of damages can fully compensate the claimant for the damage done: *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB) [236]. As was said in that case at [209], 'Once the cat is out of the bag, and the intrusive publication has occurred, most people would think there was little to gain from instituting any legal proceedings at all'.

144 *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127, 205.

145 See Rec 9–1.

146 *Beecham Group v Bristol Laboratories Pty Ltd* (1968) 118 CLR 618.

147 *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.

- 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[148] likelihood of success to justify the preservation of the status quo pending trial;
- the plaintiff is likely to suffer injury for which damages will not be an adequate remedy;[149] and
- the balance of convenience favours the granting of an injunction.[150]

12.127 In satisfying the first requirement of a prima facie case and sufficient likelihood of success, the plaintiff will already have needed to address the balancing process as part of the actionability requirements of the new tort. The public interest in freedom of expression and any other public interest would need to be addressed by the plaintiff to make out a prima facie case and to show a likelihood of success at trial on the claimed cause of action. However, the ALRC nevertheless considers that it would be valuable for the legislation to indicate the clear parliamentary intention that courts considering injunctive relief should carefully weigh the strength of the competing interests of the parties *in relation to that remedy*. In particular, such a provision would give added assurance to members of the media, who may be concerned that a statutory cause of action would unduly chill their ability to report on matters of public concern.

12.128 The ALRC is not suggesting that the legislation entrench a particular approach or weight to the competing interests of the parties. As the International Covenant on Civil and Political Rights recognises, both the individual and public interests in the protection of privacy and the individual and public interests in freedom of speech are important values and neither is absolute nor always in conflict with the other.[151] In particular, the ALRC is not suggesting any rigid or default rule that courts should be exceptionally reluctant, as in defamation cases, nor ready, as in breach of confidence cases, to grant an injunction. Those two differing types of case protect and balance different interests than those that will be protected under the new tort, even though sometimes the interests may overlap. Rather, the recommendation confirms that competing public interests are to be considered when considering an injunction application.

---

148 '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).

149 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 124, [21–345].

150 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [19] (Gleeson CJ and Crennan J); Ibid, [65]–[72] (Gummow and Hayne JJ).

151 As Ch 2 points out, privacy allows an individual to speak freely. Even in the United States it is recognised that the First Amendment protecting freedom of speech and freedom of association 'serves to protect privacy': Daniel J Solove, Marc Rotenberg and Paul M Schwartz, *Information Privacy Law* (Aspen, 2nd ed, 2006) 33.

Injunctions in defamation and breach of confidence

12.129 An applicant for an interlocutory injunction in defamation cases faces an additional hurdle in the application of the rules set out in *Beecham.*[152] This hurdle may be described as the rule in *Bonnard v Perryman,* which derives from Lord Coleridge CJ's statement 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'.[153] In particular, if a defendant asserts that it will defend the defamatory statement as true, then, 'in all but exceptional cases',[154] the courts will exercise their discretion to refuse the injunction, leaving the defendant to publish and risk liability for damages.

12.130 This caution in defamation cases is well-established in Australian law, although the defendant must go further than merely *raising* the defence.[155] 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.[156] 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'.[157]

12.131 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'.[158] The broader species to which their Honours were referring presumably comprises those cases where the disposal of the interlocutory application would effectively determine the case in its entirety, but might possibly include applications for interlocutory injunctions in the auxiliary jurisdiction in general.

---

152 *Beecham Group v Bristol Laboratories Pty Ltd* (1968) 118 CLR 618.

153 *Bonnard v Perryman* (1891) 2 Ch 269, 283–85. 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.

154 *Bonnard v Perryman* (1891) 2 Ch 269, 285.

155 *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]. However, Heydon J in dissent in *ABC v O'Neill* went so far as to say that one proposition flowed from the appeal in that case: 'That is that as a practical matter no plaintiff is ever likely to succeed in an application against a mass media defendant for an interlocutory injunction to restrain publication of defamatory material on a matter of public interest, however strong that plaintiff's case, however feeble the defences, and however damaging the defamation': *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [170].

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

157 *Australian Broadcasting Corporation v O'Neill* 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).

158 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [75].

12.132 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. The courts in both equitable and contractual cases emphasise that, when granting an injunction to restrain a breach of confidence, they are holding the defendant to his or her pre-existing commitment or obligation, usually voluntarily undertaken, not to disclose the plaintiff's confidential information. In the case of a third party, the third party is bound when they know that the information was imparted in such circumstances.[159] On many occasions, the courts have strongly emphasised the public interest in the law's upholding of confidences: if a person cannot rely on confidentiality being upheld, he or she is unlikely to impart the information. In many circumstances, withholding the information would have a deleterious effect on a range of social problems, such as public health or the prevention and detection of criminal conduct. For example, immunity from disclosure of the identity of individuals who give information to authorities about suspected neglect or ill-treatment of children is given because of the public interest served in having such conduct reported.[160]

12.133 Both in claims for breach of an *equitable* obligation of confidence, which lie in equity's exclusive jurisdiction,[161] and perhaps even more so in claims to restrain the breach of a *contractual* obligation of confidence,[162] which lie in the auxiliary jurisdiction,[163] authority in Australia takes a narrow approach to public interest considerations that would justify a breach. Public interest is confined to the exposure of 'iniquity'. 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.[164]

---

159 *Earl v Nationwide News Pty Ltd* [2013] NSWSC 839 (20 June 2013) 17.

160 *D v NSPCC* [1978] AC 171. Another example, and a rare exception to the principle of open justice, is the protection of the identity of victims of blackmail and similar offences: *R v Socialist Worker Printers and Publishers Ltd* [1975] 1 QB 637. In blackmail and analogous cases, the basic principle of open justice may be qualified if it is positively established that, without giving anonymity to an informant, justice could not be done because of the grave difficulty in having the witnesses come forward: *R v His Honour Judge Noud; Ex parte MacNamara* (1991) 2 Qd R 86, 106.

161 The exclusive jurisdiction arises where a court of equity is dealing with equitable claims: Meagher, Heydon and Leeming, above n 124, [21–015].

162 *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987) [57]. Contractual claims attract equity's auxiliary jurisdiction to restrain the breach of a negative covenant. Meagher, Heydon and Leeming, above n 124, [21–195].

163 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].

164 *Re Corrs Pavey Whiting and Byrne v Collector of Customs of Victoria and Alphapharm Pty Ltd* [1987] FCA 266 (13 August 1987) [57].

12.134 The current Australian approach differs from the much broader approach to public interest taken in the UK in such cases.[165] 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 defendant not by balancing and then overriding those demands by reference to matters of social or political opinion.[166]

12.135 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'.[167] Breach of confidence claims arise in a wide range of social and commercial contexts and the ALRC is not concerned with considering whether a broader public interest test should be introduced in breach of confidence actions in general. The issue is relevant only in relation to the impact the approach may have on the way that the courts deal with privacy claims.

Injunctions to restrain disclosure of *private* information

12.136 If the statutory cause of action were enacted, questions will inevitably arise as to what approach the courts should take where they are considering a claim for misuse or disclosure of *private* (rather than confidential) information.[168] Should 'private information' cases be seen as more analogous to defamation cases or as more analogous to 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?

12.137 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

---

165 *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 expansive approach.

166 *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].

167 *Australian Football League v The Age Company Ltd* (2006) 15 VR 419, [75]. If there is a defence of public interest to disclosure of confidential information, it may be limited in scope: *Commonwealth v John Fairfax and Sons* (1980) 147 CLR 39, 56–57.

168 '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': *Spelman v Express Newspapers* [2012] EWHC 355 (QB) (24 February 2012) [64]. See, also, Godwin Busuttil and Patrick McCafferty, 'Interim Injunctions and the Overlap between Privacy and Libel' (2010) 2 *Journal of Media Law* 1.

law.[169] It is important, therefore, that actions for invasion of privacy be treated consistently with other actions where rationales are similar.[170]

12.138 Depending on their facts, actions for invasion of privacy under the new tort would sit somewhere between defamation and breach of confidence actions. They may share some of the characteristics of both actions but differ in other ways. Like confidential information, the privacy of information once lost, may be lost forever. This is particularly so in the digital era where it is often simply not possible to erase all disclosures of private information on the internet, despite attempts and even court directions to do so.[171] A refusal to give injunctive relief to restrain the publication of private information would therefore, like that to prevent a breach of confidence, 'substantially determine the plaintiff's claim for final injunctive relief'.[172] Unlike a breach of confidence claim, however, the claim is not necessarily based on a pre-existing obligation or commitment to maintain privacy. And, in contrast to the current Australian law on breach of confidence, the new statutory cause of action would require the court to consider a broader range of public interest matters than matters which may come within the description of an 'iniquity'.

12.139 Unlike a defamation case, a defendant in a privacy case cannot assert the truth of the disclosed information as a complete defence.[173] The complaint in defamation is that the defendant has published *false* defamatory statements. Nearly all cases of invasion of privacy by wrongful disclosure in other jurisdictions involve information which might be assumed to be *true*.[174]

12.140 There is, however, just as strong and justifiable a concern that a chilling effect upon freedom of speech and the freedom of the press may be achieved by unmeritorious claims to prevent the disclosure of allegedly 'private' information in which there is a legitimate public interest. It may therefore be strongly arguable that similar considerations to those in defamation cases should apply where the defendant

169 *Sullivan v Moody* (2001) 207 CLR 562. See further Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy', above n 29, 187–190.

170 Given that the plaintiff under the new tort would be asserting a statutory wrong rather than an 'equitable' one, the court would be exercising its auxiliary or concurrent jurisdiction, rather than its exclusive jurisdiction. See Meagher, Heydon and Leeming, above n 124, 708, 714. The principles as to injunctions vary.

171 *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez* (CJEU) C‑131/12 (13 May 2014).

172 *Earl v Nationwide News Pty Ltd* [2013] NSWSC 839 (20 June 2013) [18].

173 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: Sappideen and Vines, above n 24, 635–639.

174 Just as the fact that the information is true is not a defence to an action for misuse of private information, a claimant against the misuse of private or confidential information cannot defend a claim by demonstrating that the matter is untrue. Unlike a case in defamation, the issue in such a case is whether the information is private, not whether it is true or false: *McKennitt v Ash* [2008] QB 73, [80], [86].

asserts a defence of sufficient strength to justify the court taking a cautious approach.[175]

12.141 The ALRC recommendation reflects that concern, and, without suggesting that the same approach to defamation cases should prevail, suggests that at least 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. It will be a matter for the courts as to how the balance of protection should be struck in particular cases, in the light of technological and social conditions very different from 1891 when *Bonnard v Perryman* was decided.[176] As mentioned above, the existence of such a provision would indicate a clear intention that public interest should be considered and would provide considerable assurance to media and other stakeholders concerned that the new tort would unduly impinge on freedom of speech.

12.142 The ALRC's recommendation has a similar intent to s 12(4) of the *Human Rights Act 1998* (UK), although it is in more general terms. 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,[177] s 12 provides the added protection of art 10 rights:[178]

> 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—

---

175 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 of Madingly v Associated Newspapers Ltd* [2007] EWCA Civ 295, [28] (Eady J). This concern motivated Tugendhat J in *Terry v Persons Unknown* [2010] to note 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': *Terry v Persons Unknown* [2010] EWHC 119 (QB), [88]. He dismissed the claimant's application for an injunction to restrain the publication of confidential and private information: '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'[123]. Witzleb argues that this approach is inconsistent with the requirements of the *Human Rights Act 1998* (UK): Normann Witzleb, 'Interim Injunctions for Invasions of Privacy: Challenging the Rule in Bonnard v Perryman?' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014). Cf the Australian position outlined in Rolph, 'Irreconcilable Differences? Interlocutory Injunctions for Defamation and Privacy', above n 141, 29. See, also, Busuttil and McCafferty, above n 168.

176 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57, [269]–[280] (HeydonJ).

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

178 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.

> (a) the extent to which—
>
> (i) the material has, or is about to, become available to the public; or
>
> (ii) it is, or would be, in the public interest for the material to be published;
>
> (b) any relevant privacy code.

12.143 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 have 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* noted

> [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.[179]

12.144 Similarly, 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.[180]

12.145 Section 12(2) and (3) of the *Human Rights Act 1998* (UK) provide:

> (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.

12.146 However, in the light of established principles concerning ex parte applications,[181] and the strength of the defendant's case in interlocutory proceedings,

---

179 *Campbell v MGN Ltd* [2004] 2 AC 457, [488] (citations omitted).

180 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'.

181 See, further, Meagher, Heydon and Leeming, above n 18, [21–425].

set out in *ABC v O'Neill,*[182] it is not suggested that provisions similar to s 12(2) and (3) of the *Human Rights Act* (UK) are necessary or desirable in Australia.[183]

Delivery up, destruction or removal of material

Recommendation 12–9 The Act should provide that courts may order the delivery up and destruction or removal of material.

12.147 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 be appropriate in many contexts involving both print information and online information where two people in an intimate relationship share images or text of a highly personal nature and one party intends to, or does, 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 or taken off the internet. Several stakeholders supported this recommendation.[184]

12.148 Women's Legal Services NSW argued that

> it is important that power extend to orders to take down online content. It is essential that this order bind third parties such as internet providers and organisations that run social media websites.[185]

12.149 This power should 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 in the *Copyright Act 1968* (Cth), empowering a court to order the delivery up and destruction of material which violates copyright law.[186]

12.150 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

182 *Australian Broadcasting Corporation v O'Neill* (2006) 227 CLR 57; *Beecham Group v Bristol Laboratories Pty Ltd* (1968) 118 CLR 618.

183 On the meaning of 'likely' in s 12(3), see *Cream Holdings Ltd v Banerjee* (2004) 1 AC 253, [22]. In that case, Lord Nicholls stressed that 'likely' could mean different things depending upon its context: *ETK v News Group Newspapers Ltd* (Unreported, [2011] EWCA Civ, 19 April 2011) 439, [6], [24]. In that case, the court explained, it meant 'likely in the sense of more likely than not'.

184 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 97*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*; T Gardner, *Submission 3*.

185 Women's Legal Services NSW, *Submission 115*.

186 *Copyright Act 1968* (Cth) s 133.

destruction of evidence.[187] Anton Pillar orders are issued when a court considers that a defendant is likely to destroy documents or property necessary for proceedings.[188]

12.151 The NSWLRC and ALRC[189] 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 any 'articles, documents or material (and any copies), that were made or disclosed as a result of the invasion'.[190]

12.152 Women's Legal Services NSW also submitted that, in order to facilitate access to justice, local courts should be given the power to grant stand-alone injunctive orders such as take down orders and/or deliver up orders.[191] However, there are jurisdictional difficulties and wider implications with local courts being given these powers.

12.153 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.[192] The ALRC has not proposed such an order, because such systemic problems would generally be the result of negligent acts or omissions and be more appropriately dealt with by the regulator. The new tort is confined to intentional or reckless invasions of privacy. Chapter 16 discusses ideas for a wider complaints mechanism for serious invasions of privacy that would allow the Privacy Commissioner to recommend the take down of material.

Correction orders

Recommendation 12–10 The Act should provide that courts may, where false private information has been published, order the publication of a correction.

12.154 The ALRC recommends that courts be given the power to order defendants to publish, in appropriate terms, a correction where false *private* information is published or otherwise disclosed.[193] Such an order can set the record straight, and may

187 Bernard Cairns, *Australian Civil Procedure* (Thomson Reuters (Professional) Australia, 8th ed, 2009) [13.80].

188 *Long v Specifor Publications Pty Ltd* (1988) 44 NSWLR 545, [547] (Powell JA).

189 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 74–5(f).

190 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWLRC Draft Bill, cl 76(1)(d).

191 Women's Legal Services NSW, *Submission 115*.

192 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).

193 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

be necessary where, for example, the defendant disclosed *untrue* private information about the plaintiff. This acknowledges the harm and distress which may be occasioned where false information on a personal or private nature is published.

12.155 As discussed in Chapter 5, the disclosure of private information may amount to a serious invasion of privacy despite the information being untrue.[194] 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.[195]

12.156 Correction orders may reduce the need for a plaintiff's interests to be vindicated through an award of damages.[196] Some plaintiffs may be primarily concerned with correcting the public record, in which case correction orders should target the same audience. Carroll and Witzleb have made the point that in actions to restore personality interests, monetary remedies may be ill-suited.[197] 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.

12.157 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.[198] 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.[199]

12.158 Guardian News raised the concern that correction orders will 'constitute a further and unnecessary restriction on free speech'.[200] Similarly, the ABC was concerned that court-ordered apologies and correction orders could inhibit the editorial independence of journalists.[201] These news organisations were concerned that the

---

into account when assessing the 'reasonableness' of any offer of amends, for example in *Defamation Act 2005* (NSW) 2005 s 14.

194 See Ch 5.

195 *McKennitt v Ash* [2008] QB 73, 86.

196 Carroll and Witzleb, above n 17, 236.

197 Ibid, 233.

198 ASTRA, *Submission 47*.

199 See Rec 12–2.

200 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

201 ABC, *Submission 93*.

availability of these remedies will chill media activities, causing journalists to become reluctant to publish news items which may contain *private* information. However, the availability of a correction order will only arise in instances where the defendant published private information which was false and which was a serious invasion of privacy. This is consistent with anti-discrimination law. For instance, in *Eatock v Bolt* Bromberg J noted that the purposes a corrective notice can serve to facilitate are:

> redressing the hurt felt by those injured; restoring the esteem and social standing which has been lost as a consequence of the contravention; informing those influenced by the contravening conduct of the wrongdoing involved.[202]

12.159 There may be instances where a plaintiff would not wish a public correction of false private information to be made—in circumstances where that plaintiff feels the order would compound the hurt, distress or embarrassment occasioned by the original publication. This will be a matter for the plaintiff in a given case.

Apology orders

Recommendation 12–11 The Act should provide that courts may order the defendant to apologise.

12.160 The purpose of a plaintiff seeking an order for the defendant to apologise—either in private or public—will differ depending on the circumstances of the case. The availability of an order requiring a defendant to apologise may, in some circumstances, vindicate the hurt and distress caused to a plaintiff by a serious invasion of privacy.[203] Given the aim of the new 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.

12.161 In many cases, a plaintiff may only seek a public acknowledgment of wrongdoing as a remedy for a serious invasion of privacy. The publicity garnered by a public statement of apology may help to 'restore the esteem and social standing which has been lost as a consequence of the contravention'.[204]

12.162 Carroll and Witzleb have argued that orders for apology help to 'redress the injury by restoring the plaintiff's dignity and personality'.[205] Similarly, Professor 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.[206]

---

202 *Eatock v Bolt (No 2)* (2011) 284 ALR 114, [15].

203 Several stakeholders supported this proposal: N Witzleb, *Submission 116*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Insurance Council of Australia, *Submission 15*; I Pieper, *Submission 6*; I Turnbull, *Submission 5*.

204 *Eatock v Bolt (No 2)* (2011) 284 ALR 114, [15].

205 Carroll and Witzleb, above n 17, 237.

12.163 Orders for apologies also serve a public interest in focusing on the defendant's wrongdoing. In this way, public apologies provide an opportunity for a defendant to acknowledge their wrongdoing. Public apologies will therefore carry some deterrent effect and may also serve to educate the public about privacy.[207]

12.164 The ALRC previously recommended that courts be empowered to order a defendant to apologise.[208] 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.[209] The Victorian Law Reform Commission (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.[210]

12.165 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.[211] For example, a court may order an apology under Commonwealth and state anti-discrimination legislation.[212] 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.[213] 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'.[214]

12.166 Apology orders are available in some Australian jurisdictions under existing privacy legislation, for example under s 55(2)(e) of the *Privacy and Personal Information Protection Act 1998* (NSW). In *NZ v Director, Department of Housing*,[215] the NSW Administrative Appeals tribunal ordered—under s 55(2)(e)—the Department of Housing to provide written apology to the claimant for disclosing private information to a third party without consent.

---

206 Prue Vines, 'The Power of Apology: Mercy, Forgiveness or Corrective Justice in the Civil Liability Arena?' (2007) 1 *Public Space* 1, 15.

207 Carroll, above n 6, 339.

208 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–5(d).

209 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) NSWLRC Draft Bill, cl 74(3)(a)(vi).

210 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [7.207].

211 Carroll, above n 6, 213.

212 See, eg, *Federal Court of Australia Act 1976* (Cth) s 23. 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. Analogous provisions exist in other jurisdictions: *Anti-Discrimination Act 1991* (Qld) s 209. Apologies made by respondents in personal injury matters are not treated as evidence of admission of fault: *Civil Liability Act 2002* (NSW) s 69.

213 See, eg, *Defamation Act 2005* (NSW) 2005 s 38.

214 *Burns v Radio 2UE Sydney Pty Ltd (No 2)* [2005] NSWADTAP 69 (6 December 2005).

215 *NZ v Director, Department of Housing* [2006] NSWADT 173 (7 June 2006).

12.167 Several media organisations and representative groups opposed this proposal.[216] ASTRA opposed any remedy that would allow for apologies or corrections, arguing that existing provisions in the ASTRA Codes, which are subject to enforcement by the ACMA offer sufficient remedies in the context of subscription broadcasting. However, they argued that this remedy could be applied to non-media defendants who are not subject to the ACMA's code of conduct.[217] ASTRA and Guardian News also argued that, where there has been a serious invasion of an individual's privacy, discussion of the relevant information may result in further harm to the individual concerned rather than being an effective remedy. However, if this were the case, the plaintiff would not seek the remedy.

12.168 As with correction orders, the ABC and Guardian News were concerned that apology orders would inhibit editorial independence.[218] Similarly, Guardian News argued that 'requiring media organisations to correct or apologise will constitute a further and unnecessary restriction on free speech'.[219] However, the remedy would only be one of many available remedies and in any event it can only be considered where the plaintiff has made out a serious, unjustifiable, intentional or reckless invasion of privacy.

12.169 A court may order a public or private apology, depending on the circumstances of a case. For an apology to be sincere and meaningful, a court will not compel an apology where a defendant makes clear they offer no remorse and therefore their apology will not come freely.[220]

12.170 Apology orders, like all court-ordered remedies, are coercive in nature and, if breached, constitute contempt of court. Some legislation anticipates breaches of apology orders by providing that orders must be met within a specified period subject to a fine.[221]

Declarations

Recommendation 12–12 The Act should provide that courts may make a declaration.

12.171 The availability of declaratory relief will provide plaintiffs with a sense of certainty and may avoid lengthy and costly court proceedings.[222] Several stakeholders

216 ASTRA, *Submission 99*; ABC, *Submission 93*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.
217 ASTRA, *Submission 99*.
218 ABC, *Submission 93*.
219 Guardian News and Media Limited and Guardian Australia, *Submission 80*.
220 *Eatock v Bolt (No 2)* (2011) 284 ALR 114, [50] (Bromberg J).
221 See, eg, *Anti-Discrimination Act 1977* (NSW) s 108(7).
222 Meagher, Heydon and Leeming, above n 124, [19–180].

supported the availability of declaratory relief in an action for serious invasion of privacy.[223]

12.172 In a declaration in an action for serious invasion of privacy a court may state the nature of the interests, rights or duties of the applicant to an action.[224] A declaration may provide both parties to a proceeding with clarity as to their obligations and rights to avoid 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'.[225]

12.173 Declarations are available in a variety of areas of Australian law.[226] 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.[227] The Australian Competition and Consumer Commission has sought declarations under this provision in numerous cases to determine whether a party has violated Australian consumer law.[228] Declarations are also available in anti-discrimination law.[229]

12.174 The ALRC, NSWLRC and VLRC previously proposed that courts be able to make declarations.[230]

12.175 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) provides the ACMA with the power to accept undertakings from broadcasters on a range of matters.

12.176 However, the ALRC considers that the availability of declaratory relief could have a significant impact on the conduct of a defendant, given the risk of monetary remedies if legal rights which have been the subject of a judicial pronouncement are contravened.

---

223 T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; Public Interest Advocacy Centre, *Submission 30*; N Witzleb, *Submission 29*.

224 Cairns, above n 187, [1.20].

225 *Bass v Permanent Trustee Co Ltd* (1999) CLR 198 334, [356] (Gleeson CJ, Gaudron, McHugh, Gummow, Hayne and Callinan JJ).

226 Meagher, Heydon and Leeming, above n 124, [19–075].

227 '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': *Federal Court of Australia Act 1976* (Cth) s 21.

228 *Australian Competition & Consumer Commission v Black on White Pty Ltd* [2001] FCA 187.

229 For example, declaratory relief was issued in *Eatock v Bolt (No 2)* (2011) 284 ALR 114.

230 Australian Law Reform Commission, *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) NSWLRC Draft Bill, cl 76(1)(c); Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) rec 29(c).

Costs

12.177 Generally, a successful plaintiff is entitled to receive party and party costs, in the absence of countervailing circumstances.[231] The ALRC considers that a court hearing a claim for serious invasions of privacy should have discretion in relation to awards of costs. The ALRC considers that two options would be appropriate for inclusion in legislation enacting the new tort on the court's power with respect to awards of costs.

12.178 The first option would for the legislation to include a provision similar to s 43(2) of the *Federal Court of Australia Act 1970* (Cth), which provides that, '[e]xcept as provided by any other Act, the award of costs is in the discretion of the Court or Judge'.

12.179 Section 43 then provides for a range of orders that a judge may make, including:

> (3) Without limiting the discretion of the Court or a Judge in relation to costs, the Court or Judge may do any of the following:
>
> make an award of costs at any stage in a proceeding, whether before, during or after any hearing or trial;
>
> make different awards of costs in relation to different parts of the proceeding;
>
> order the parties to bear costs in specified proportions;
>
> award a party costs in a specified sum;
>
> award costs in favour of or against a party whether or not the party is successful in the proceeding;
>
> order a party's lawyer to bear costs personally;
>
> order that costs awarded against a party are to be assessed on an indemnity basis or otherwise.

12.180 This recommendation relates to party and party costs which are those costs that a court may order a party to a proceeding to pay to the other party.[232] Party and party costs must be reasonable and necessary for the proper conduct of a case.[233]

12.181 In its report, *Costs Shifting—Who Pays for Litigation*, Report 75 (1995) (*Costs Shifting)*, the ALRC identified several reasons for the award of costs to a successful plaintiff:

- to compensate successful litigants for at least some of the costs they incur in litigating;
- to allow people without means to litigate;
- to deter vexatious or frivolous or other unmeritorious claims or defences;

---

231 *Hughes v Western Australian Cricket Association (Inc)* [1986] FCA 382.

232 *Civil Procedure Act 2005* (NSW) s 98; *Supreme Court Act 1986* (Vic) s 24; *Rules of the Supreme Court 1971* (WA) O 66 r 1; *Court Procedure Rules 2006* (ACT) r 1721; *Local Court Rules* (NT) r 63.03.

233 Cairns, above n 187, [17.80].

- to encourage settlement of disputes by adding to the amount at stake in the litigation; and
- to deter delay and misconduct by making the responsible party pay for the costs his or her opponent incurs as a result of that delay or misconduct.

12.182 The second option would be for the legislation to provide that awards of costs should be determined according to the enabling act of each court or tribunal that is given jurisdiction to hear the action. This would have the advantage that plaintiffs could consider the court or tribunal's particular powers with respect to costs when deciding on an appropriate forum to bring their action.

12.183 The manner in which costs are awarded is critical to providing appropriate access to justice—a principle that informs the work of this Inquiry.[234] Access to justice was raised by several stakeholders who argued that the principle should underscore much of the ALRC's formulation of the new tort.[235]

12.184 The forum in which a statutory cause of action is to be heard will impact on the potential award of costs. The ALRC deals with the matter of forums for the cause of action in Chapter 10, recommending that federal courts and appropriate state and territory courts would have jurisdiction to hear actions under the new tort. The ALRC has not recommended that the new tort be heard in state tribunals such as VCAT,[236] although the ALRC leaves this possibility open.

12.185 Several submissions raised the concern that many plaintiffs may be deterred from starting proceedings due to the risk of an adverse costs order.[237] 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. PIAC argued that,

> in the absence of such a costs rule, there is a risk that privacy-related litigation 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 in the event they are unsuccessful. In PIAC's experience, even where pro bono legal representation or representation on a conditional fee basis is secured, many meritorious cases do not proceed due to the risk of an adverse costs order. This is especially the case in matters where there is a great disparity in resources between the applicant and respondent.[238]

---

234 The OAIC's submission raised costs as an issue which influences the accessibility of civil proceedings: Office of the Australian Information Commissioner, *Submission 66*.

235 ACCAN, *Submission 106*; Public Interest Advocacy Centre, *Submission 105*; Office of the Australian Information Commissioner, *Submission 90*.

236 The VLRC recommended that costs be dealt with in accordance with s 130 of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic). 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. This approach was supported by the Office of the Victorian Privacy Commissioner in their submission to the Discussion Paper.

237 Redfern Legal Centre, *Submission 46*; Public Interest Advocacy Centre, *Submission 30*.

238 Public Interest Advocacy Centre, *Submission 105*.

12.186 Similarly, Redfern Legal Centre proposed the adoption of an adverse costs model similar to that operating in employment law in Australia.[239] Under s 570(2)(a) of the *Fair Work Act 2009* (Cth), costs incurred in a proceeding in any court will only be awarded against an unsuccessful plaintiff if the proceedings are vexatious or unreasonable. Redfern Legal Centre argued that privacy complaints were analogous to proceedings under that Act rather than any commercial proceedings.[240]

12.187 The ALRC notes stakeholder concerns about the deterrent effect of potentially adverse costs orders. The ALRC supports the principle of broad access to justice, but notes that costs orders are also designed to deter vexatious or unmeritorious claims.[241] The ALRC considers that actions for serious invasion of privacy should be dealt with consistently with actions brought in the forum for other intentional torts or other analogous actions.

12.188 Women's Legal Services NSW and the Australian Institute of Professional Photography (AIPP) suggested a court should be empowered to award indemnity costs where a defendant has demonstrated malice or vindictiveness.[242] Unlike party-party costs which operate as a partial indemnity for the successful party against liability for legal costs,[243] indemnity costs, which fully compensate the successful party for the inappropriate conduct of another party to the proceedings, are only awarded in exceptional circumstances.[244] Most courts have the power to award indemnity costs in lieu of party-party costs in appropriate circumstances.

239 Redfern Legal Centre, *Submission 94*.
240 Ibid.
241 Insurance Council of Australia, *Submission 102*.
242 Women's Legal Services NSW, *Submission 115*; Australian Institute of Professional Photography (AIPP), *Submission 95*.
243 Cairns, above n 187, [17.80].
244 Ibid [17.190].

Part 3

13. Breach of Confidence Actions for Misuse of Private Information

Contents

Summary 263
The likely future development of the action for breach of confidence 264
Compensation for emotional distress 265
- Remedies for breach of confidence 266
- Emotional distress: a common result of misuse of private information 268
- Why the law needs clarification 269
- Stakeholder views 270
- The case for compensation for emotional distress 272

Public interest and injunction applications 273

Summary

13.1 In addition to 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.

13.2 In the event that the statutory cause of action is not enacted, the ALRC recommends that courts be empowered by legislation to award compensation for emotional distress in cases involving disclosure of private information.[1]

13.3 The recommendation aims, first, to address existing uncertainty as to whether Australian law provides a remedy for emotional distress suffered as a result of the

1 With regard to intrusion into seclusion, the other type of invasion included in the statutory tort, the ALRC considers that if a statutory cause of action for serious invasion of privacy is not enacted, a statutory action for protection against harassment would be a more targeted or limited way for the law to be developed: this is discussed in Ch 15. Ch 3 considers the possibility of the common law developing a tort of harassment or a tort of invasion of privacy by intrusion into seclusion. It would be necessary for the courts 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 included emotional distress.

disclosure or misuse of private information,[2] and secondly, to ensure that the law does provide such a remedy.

13.4 This would be a limited and targeted way in which the law could be amended to provide greater redress for serious invasions of privacy and to fill a significant gap in the existing law.

13.5 This chapter begins with a brief section on the likely future development of the breach of confidence action. It then sets out the case for the recommendation. It concludes with an explanation of why the ALRC does not proceed with a proposal made in the Discussion Paper which related to public interest considerations in applications for injunctions to restrain the publication of private information.

The likely future development of the action for breach of confidence

13.6 In Chapter 3, the ALRC sets out the existing legal protection of an individual's privacy, and notes the consensus of both courts and commentators that the course of the likely future development of the common law in this area is still uncertain.

13.7 In *ABC v Lenah Game Meats,* the court suggested that existing legal actions may be extended to protect against invasions of privacy. Gummow and Hayne JJ, with whom Gaudron J agreed, considered a broad 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 … 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.[3]

13.8 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:

---

2 This recommendation 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, [110], [132]. Citing the American Law Institute, *Restatement of the Law of Torts (Second)* (1977), 2d § 652A, Comment b.

> [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.
>
> 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.[4]

13.9 Despite the influential and open invitation by the High Court to the lower courts to develop further protection, there has been only isolated development of further privacy protection in Australia at common law, as discussed in Chapter 3, making it difficult to predict the precise direction of future developments.[5]

13.10 Nevertheless, this chapter assumes 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 misuse and disclosures of private information.[6]

Compensation for emotional distress

Recommendation 13–1 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 plaintiff's emotional distress.

---

4 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [34], [39], [40], [55].

5 'The recent High Court of Australia decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* does little to clarify the future direction of Australian jurisprudence': *Hosking v Runting* (2005) 1 NZLR 1, [56]–[59] (Gault P and Blanchard J).

6 The alternative way for the common law to develop greater protection would be to recognise a new tort, as in New Zealand. See further Ch 3.

13.11 There are several arguments in favour of the ALRC's recommendation for compensation for emotional distress. First, if legislation clarified or confirmed that equitable compensation[7] 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 plaintiffs.[8] This is particularly important in the event that the statutory cause of action is not enacted.

13.12 Secondly, the effectiveness and availability of the remedy may deter invasions of privacy involving disclosures of private information.

13.13 Thirdly, this recommendation 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.

13.14 Fourthly, this provision would indicate that Australian legislatures intended that the action for breach of confidence could be relied on to remedy these kinds of invasions of privacy.

Remedies for breach of confidence

13.15 In traditional claims for breach of confidence in Australia, plaintiffs have generally sought one of three remedies: an injunction to restrain an anticipated or continuing breach of confidence; an account of the anticipated profits derived from a breach; or compensation for economic loss due to a breach.

13.16 An injunction to restrain publication or misuse is the most valuable and effective remedy in respect of all kinds of information: commercial, governmental or personal information. The remedies of an account of profits or equitable compensation are usual in cases involving commercial information. Beginning with Prince Albert suing to restrain the publication of a catalogue of Queen Victoria's family etchings in 1849,[9] breach of confidence actions in equity have long been used to protect personal information, but the cases invariably concerned applications for injunctions.[10]

---

7 The term 'equitable compensation' here is used to refer to an award of monetary compensation in an equitable action. 'Equitable compensation' has become the standard term for equitable monetary relief awarded for loss suffered by reason of breach of a purely equitable obligation—that is, in the exclusive jurisdiction': Dyson Heydon, Mark Leeming and Peter Turner, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2014) [23–015]. The authors distinguish 'damages' which are awarded in common law actions, including under *Lord Cairns' Act.* See also the 'Remedies' section of Chapter 42 'Confidential Information' of the same book; and *The Salvation Army (South Australia Property Trust) v Rundle* [2008] NSWCA 347.

8 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.'

9 *Prince Albert v Strange* (1849) 1 Mac G 25.

10 Public Interest Advocacy Centre, *Submission 105*. See also *Stephens v Avery* [1988] Ch 449, 454; *Argyll v Argyll* (1965) 1 ER 611; *Lennon v News Group Newspapers Ltd* [1978] FSR 573.

Compensation for breach of confidence

13.17 While the general entitlement to compensation for breach of confidence is now well-established, issues about assessment remain unresolved. In 1982, IE Davidson noted that, even in commercial cases, assessment of loss was difficult:

> The 'protean quality of information' makes it difficult to estimate what is required to finally restore a plaintiff to his position prior to the breach of his confidence. Nevertheless, relief based on the value for which the information would be sold between a willing buyer and a willing seller seems to be a satisfactory general criterion. There may be more serious difficulties in using Equity's compensatory jurisdiction to remedy breaches of personal confidence where the damage suffered by the discloser through the confidant's breach of duty will rarely be directly measurable in financial terms. Compensation, being based on specific restitution for the value of what has been lost, seems more appropriate for recovering identifiable financial loss or specific property than for granting solatium for personal suffering or loss of reputation caused by breach of a personal confidence. Whilst compensation may have a role, the major scope for a principled development of techniques with which to remedy losses due to breach of this equitable duty will be where the confidential information had a commercial value.[11]

13.18 In 1999, the New South Wales Court of Appeal was still describing equitable compensation as 'a developing area of the law'.[12] In 2014, the authors of *Meagher Gummow and Lehane's Equity: Doctrines and Remedies* state:

> Monetary awards for loss, or something like loss, are awarded in a variety of contexts in equity. 'Equitable compensation' has come to denote many of these. It has become a category of concealed multiple reference: no single formulation can accurately describe all the applications of this relief.[13]

13.19 In cases involving confidential personal or private information, the plaintiff's economic losses or the defendant's profits would seem to be readily recoverable where the private information had a commercial value. Where it does not have a commercial value, the plaintiff may nevertheless have suffered economic loss, such as the cost of hiring a public relations consultant to manage resultant publicity, or loss of employment. A plaintiff may also suffer some other type of harm such as personal injury or psychiatric injury but there is a dearth of authority on whether such damage is recoverable.[14]

---

11 Ian Davidson, 'The Equitable Remedy of Compensation' [1982] *Melbourne University Law Review* 349, 396.

12 *Beach Petroleum NL v Kennedy* (1999) 48 NSWLR 1, [431]. See also, Heydon, Leeming and Turner, above n 7, [23–020].

13 Heydon, Leeming and Turner, above n 7.

14 Authorities denying claims for personal injury based on fiduciary duties turn on the absence of a fiduciary obligation to protect that type of interest. See also, Ibid [23–605]. Recovery of common law damages in contractual cases depends on remoteness principles: see eg, *Cornelius v de Taranto* [2001] EMLR 12; *Archer v Williams* [2003] EWHC 1670 (QB).

Emotional distress: a common result of misuse of private information

13.20 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 plaintiff is most likely to suffer is emotional distress. 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'.[15]

13.21 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'.[16]

13.22 It is well-established that tort law allows recovery of compensation for 'mere' emotional distress, even intentionally caused, in only limited circumstances.[17] The issue of whether compensation for emotional distress can be awarded in equity was first raised in Australia in *Giller v Procopets.*[18] Neave JA of the Supreme Court of Victoria Court of Appeal noted: '[t]he Australian position appears to be at large on this issue. I am not aware of any appellate court decision which has considered it.'[19]

13.23 Allowing the plaintiff's appeal, the court in *Giller v Procopets* held that the plaintiff 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 plaintiff and defendant while in a de facto relationship. The court unanimously agreed that the plaintiff could recover compensation for her consequent emotional distress as equitable compensation.[20] An application by the defendant to the High Court for leave to appeal was rejected.[21]

---

15 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.

16 Law Institute of Victoria, *Submission 22*.

17 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 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 J Edelman, J Goudkamp and S Degeling (eds), *Torts in Commercial Law* (Thomson Reuters, 2011).

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

19 Ibid [419]. See also Ashley JA at [133].

20 Neave JA, with whom Maxwell JA agreed, also supported the award as damages under the Victorian equivalent of *Lord Cairns' Act*: s 38 of the *Supreme Court Act 1986* (Vic). 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

Why the law needs clarification

13.24 It is desirable for legislation to clarify the courts' powers to award compensation for emotional distress, notwithstanding the judgment in *Giller v Procopets,* for several reasons.

13.25 First, at the time of this Report, *Giller v Procopets* remains the sole appellate authority for the recovery of compensation for emotional distress in a breach of confidence action. 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.[22] The case was settled before appeal.

13.26 Secondly, the basis on which equity can award compensation, by way of common law compensatory damages and aggravated damages, for emotional distress arising from the breach of a purely equitable wrong remains unclear, even if *Lord Cairns' Act* or s 38 of the *Supreme Court Act 1986* (Vic) does apply. It is problematic to have a grant of equitable compensation or 'damages' by analogy with tort law, when, as Ashley JA pointed out, 'with few exceptions, the common law has turned its face against awards of damages for distress'.[23] This is even more so when, 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,[24] although that argument could also be made.[25] Rather it is an argument that the law would be

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. Section 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' Act* in other jurisdictions, where there is still controversy as to whether *Lord Cairns' Act* applies in aid of purely equitable rights such as breach of confidence: *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]. The authors in Tanya Aplin et al, *Gurry on Breach of Confidence* (Oxford University Press, 2nd ed, 2012) [19.11] state 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 [19.15] and *Cadbury Schweppes v FBI Foods* [2000] FSR 491.

21 *Procopets v Giller (M32/2009)* [2009] HCASL 187.

22 *Doe v Australian Broadcasting Corporation* [2007] VCC 281, [186].

23 *Giller v Procopets* (2008) 24 VR 1, [141].

24 '[A]cceptance 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.': Aplin et al, above n 20, [17.13].

25 Meagher, Heydon and Leeming, above n 20, [2–145] 59.

more coherent if there was legislative clarification that equitable compensation could be awarded for emotional distress where private information was misused, published or disclosed.

13.27 Thirdly, there is an unsettling lack of precedent for the award of equitable compensation for emotional distress decision, other than the decision in *Giller v Procopets*. The ALRC has been unable to find any other precedent for the award of compensation for emotional distress in a purely equitable claim.[26] Further, the decision 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.[27] The courts of the United Kingdom, starting with *Campbell v MGN Ltd* in 2004, have routinely awarded damages for emotional distress in the so-called 'extended' action of breach of confidence which protects against disclosures of private information. However, these awards 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.

13.28 It may be argued that the remedial flexibility of equity allows the award of compensation for emotional distress without the need for a precedent, provided that the award consistent with broad equitable principles and doctrines.[28] 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*[29]] thus has no common law counterpart.[30]

13.29 In a similar vein, Meagher, Gummow and Leeming refer to equity's 'inherent flexibility and capacity to adjust to new situations by reference to mainsprings of the equitable jurisdiction.'[31]

13.30 Notwithstanding these general statements, the ALRC considers that legislative clarification is desirable, as it would make the basis for an award clear and certain.

Stakeholder views

13.31 Most stakeholders who responded to the Discussion Paper commented on issues relating to the statutory cause of action or regulatory reforms rather than on the proposals that dealt with limited ways to supplement the common law. Comments on

---

26 Cf cases based on a contractual obligation: *Cornelius v de Taranto* [2001] EMLR 12. See further, B McDonald, 'Defences to Privacy: Transformation, Fault, and Public Interest' in J Goudkamp, F Wilmott-Smith and A Dyson (eds), *Tort Defences* (Hart Publishing, 2014).

27 *Harris v Digital Pulse Pty Ltd* (2003) 56 NSWLR 298.

28 *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).

29 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 216.

30 *Roads and Traffic Authority of New South Wales v Dederer* (2007) 324 CLR 330, [57] (emphasis added).

31 Meagher, Heydon and Leeming, above n 20, 415 [12–045].

this proposal varied. Those stakeholders who saw no gaps in existing law or regulation, or who considered that their industry was already over regulated, opposed the proposal,[32] or argued that such a development should be left to the courts.[33]

13.32 Guardian News and Media Limited and Guardian Australia, for example, submitted that

> [I]t would be preferable for the proposed statutory cause of action to be introduced rather than the modification of an existing cause of action. Attempts to 'shoehorn' an established action to cover an adjacent or similar situation result in the twisting of the original cause of action and fail to appropriately balance the relevant interests.[34]

13.33 The Australian Privacy Foundation supported the proposal. It submitted that it would be desirable whether or not the statutory cause of action were enacted, and that it should not be confined to private information but extend to any breach of confidence action.[35] The ALRC does not agree with these additional points. A recommendation that extended to non-private confidential information would exceed the ALRC's Terms of Reference, and would have far–reaching implications for commercial actions generally. If the cause of action for serious invasions of privacy is enacted, the recommendation, which is aimed at filling a gap in the existing law, would be unnecessary.

13.34 Other stakeholders supported the proposal in the event that the statutory cause of action was not enacted.[36] The Office of the Victorian Privacy Commissioner supported the proposal, submitting that

> This would clarify the current common law position and strengthen an action for breach of confidence.[37]

13.35 David Day also submitted that the proposal should not be seen as an alternative to a statutory cause of action, but as a 'minor amendment to existing law that would offer limited improvement to privacy protection'.[38]

---

32 ASTRA, *Submission 99*; Australian Bankers' Association, *Submission 27*. ASTRA also noted in its submission that public interest should be considered when assessing compensation for emotional distress. As noted above, there is currently no broad 'public interest' defence to breach of confidence actions in Australia.

33 Free TV, *Submission 109*. In its submission to the Discussion Paper, Telstra stated: 'Consistent with our previous submission, we do not believe damages should be awarded for emotional distress.' In its submission to Issues Paper 43, Telstra commented: 'if a significant increase in invasion or breach of privacy claims does occur in the future, as Gummow and Hayne JJ noted in *Lenah*, the adaptation and development of recognised causes of action to meet new situations and circumstances may be the most appropriate method of addressing this issue.' From this the ALRC infers that Telstra thinks the issue should be left to the courts to decide: Telstra, *Submission 107*; Telstra, *Submission 45*.

34 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

35 Australian Privacy Foundation, *Submission 110*.

36 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; T Butler, *Submission 114*; Public Interest Advocacy Centre, *Submission 105*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; Women's Legal Services NSW, *Submission 76*.

37 Office of the Victorian Privacy Commissioner, *Submission 108*.

38 D Day, *Submission 72*.

The case for compensation for emotional distress

13.36 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. As Neave JA has noted, '[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'.[39]

13.37 A remedy for emotional distress may have a powerful normative effect in the prevention of serious invasions of privacy by way of misuse or disclosure of private information. This is particularly relevant in light of the ease with which private information may be disclosed or distributed using new communication technologies.

13.38 Internet and other digital communication technology has enabled widespread and sometimes irreversible disclosures of private information causing continuing and serious harm and distress. As Gleeson CJ said in *ABC v Lenah Game Meats Pty Ltd*, citing the significant privacy concerns raised by advances in technology, '[t]he law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy'.[40]

13.39 It may well be that courts will arm themselves with the power by following the lead of *Giller v Procopets*. However, the position would be rendered more certain, and there would be less room for 'doctrinal angst',[41] argument and costly or risky litigation along the way, if legislation were the source of that power. Some stakeholders agreed that the issue of recovery of compensation for emotional distress 'remains unnecessarily complex and uncertain'.[42] It is therefore highly desirable that there be legislative clarification.

13.40 Legislation also has the advantage over common law development that it may be carefully crafted, if thought necessary, to deal with only the most egregious cases of breach of confidence concerning misuse, disclosure or publication of private information. While equitable liability for breach of confidence is conscience-based, a breach of confidence can be committed without any intent to harm, once the defendant has knowledge of the confidential nature of the information.[43] The same approach may be taken with regard to private information, whether or not it is also confidential.

13.41 The ALRC notes also that it may be appropriate to limit the remedy of compensation for emotional distress caused by disclosures of private information to the most egregious cases, such as where the disclosure was done intentionally, recklessly or even maliciously.

---

39 *Giller v Procopets* (2008) 24 VR 1, [424]. Cf Ibid [168]–[169] (Gillard J).

40 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 225, [40].

41 D Butler, *Submission 74*. '[A]ny discussion of the application of the remedy of damages in breach of confidence cases is fraught with difficulty at the outset': Aplin et al, above n 20, [19.02].

42 Australian Privacy Foundation, *Submission 110*.

43 *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] 1 WLR 1556. See also, McDonald, 'Defences to Privacy: Transformation, Fault, and Public Interest', above n 26.

Public interest and injunction applications

13.42 In the Discussion Paper, the ALRC proposed that legislation be enacted to require a court to give particular consideration to countervailing public interests, including freedom of expression, when considering an application for an injunction to prevent publication of private information, where there was not an added element of confidentiality.[44]

13.43 It was suggested that such a proposal would be desirable if the statutory tort were not enacted, and if, instead, greater protections against disclosure of (merely) private information were to develop at common law by way of the extension of the equitable action for breach of confidence.

13.44 To a certain extent, the proposal rested on an assumption that the likely development of the law would be along the lines of the development in the United Kingdom. The proposal suggested a way of directing the future development of the law. It assumed familiarity with the differences between the current law in the United Kingdom, which includes a similar provision in its *Human Rights Act 1998* (UK), and the current Australian law on breach of confidence.

13.45 The background to the proposal was the lack of clarity, which persists, about the principles that should govern the exercise of the court's discretion in any action to protect private information: would a court take an approach similar to that in breach of confidence cases or to that in defamation cases?

13.46 Australian case law provides only a very limited role for public interest considerations as a justification for restraining publication in breach of an obligation of confidence.[45] Injunctions are readily awarded to restrain the breach of a negative covenant, such as a promise not to breach confidence by revealing confidential information. The courts stress in such cases that there is an important public interest in the law holding a person to an obligation of confidence that they undertook or knew about: people will not volunteer information, even where it is in the public interest that they should do so,[46] if they feel the confidence will not be respected and enforced.

13.47 By contrast, defamation law incorporates well-established principles that protect freedom of speech, so that it is very difficult to obtain an injunction to restrain a defamatory publication if the defendant puts up a serious argument that it can be justified.[47]

13.48 The ALRC did not propose any legislative change to the way in which courts approach traditional breach of confidence cases. Rather, the ALRC's proposal was that

---

44 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) Proposal 12–2.

45 This is in contrast to the law of the United Kingdom on breach of confidence which accepts a broader defence of public interest. Yet even in the UK, there is debate about how privacy and defamation cases intersect: see further Ch 12.

46 For example, about contagious diseases or substance abuse or suspicions of abuse or corruption.

47 See Ch 12.

there should be explicit consideration required of freedom of speech and other public interests in applications to prevent the publication of information which is deemed to be *private*—but which was not subject to an obligation of confidence.

13.49 Some stakeholders were in favour of the proposal, expressing concern at the narrow defence of public interest in Australia to breach of confidence actions or at the chilling effect of injunctions on freedom of speech. However, most stakeholders concentrated on other issues in the Discussion Paper. After discussions and consultations with members of the legal profession and the judiciary about this proposal, the ALRC concludes that it may be premature to attempt to direct the approach of the common law as proposed. Therefore, the ALRC does not make any recommendation in the Final Report with respect to injunctions where the plaintiff relies on the common law to protect private information.[48]

13.50 The ALRC considers the desirability of a legislative provision with respect to injunction applications under the new tort in Chapter 12**.**

48 See further, Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (2014) 158–193.

14. Surveillance Devices

Contents

Summary	275
Existing surveillance device laws	276
A Commonwealth Act	278
Technology neutral surveillance legislation	282
Telecommunications surveillance	285
Participant monitoring	286
Responsible journalism and the public interest	289
Workplace surveillance	293
Remedial relief and compensation	295
Alternative forums for complaints about surveillance	296

Summary

14.1 In this chapter, the ALRC sets out recommendations regarding the surveillance device laws and workplace surveillance laws of the Australian states and territories. These surveillance device laws provide important privacy protection by creating offences for the unauthorised use of listening devices, optical surveillance devices, tracking devices, and data surveillance devices.

14.2 However, there is significant inconsistency in the laws with respect to the types of devices regulated and with respect to the offences, defences and exceptions. This inconsistency results in uncertainty and complexity, reducing privacy protection for individuals and increasing the compliance burdens for organisations.

14.3 A key recommendation in this chapter is that the surveillance device laws should be the same throughout Australia. The ALRC recommends that this be achieved through Commonwealth legislation. The ALRC also recommends that workplace surveillance laws be made uniform throughout Australia.

14.4 Surveillance legislation should also be technology neutral, so that it can apply to new devices, such as unmanned aerial vehicles (drones), as well as to surveillance technologies which are not 'devices' in the traditional sense, such as software or networks of devices.

14.5 The ALRC recommends the repeal of 'participant monitoring' exceptions. These exceptions allow the use of a surveillance device without the consent of the individuals under surveillance, so long as the person conducting the surveillance is also a party to the activity or conversation under surveillance.

14.6 Recognising that the participant monitoring exceptions provide protection for several important activities, the ALRC recommends a 'responsible journalism' defence that would protect journalists and media groups making appropriate use of a surveillance device for certain matters in the public interest.

14.7 Further recommendations include that compensation be available to victims of surveillance offences, and that avenues should be made available for residential neighbours to have disputes about the use of surveillance devices heard by appropriate lower courts and tribunals. The latter recommendation recognises that criminal offences may be inappropriate for some uses of surveillance devices, and that a quicker, cheaper and less onerous process may achieve the desired result of preventing invasions of privacy.

Existing surveillance device laws

14.8 Laws exist in each state and territory to regulate the use of surveillance devices.[1] These laws provide criminal offences for conducting surveillance and for related activities, in particular for communicating information obtained under surveillance. The laws also provide for the application for, and issue of, warrants to conduct surveillance by law enforcement officers; monitoring and oversight mechanisms; public interest exceptions; conditions for the admissibility of information obtained under surveillance as evidence; and restrictions on the manufacture and supply of surveillance devices. Other laws in the ACT, NSW and Victoria regulate the use of surveillance in the workplace.[2]

14.9 Surveillance device laws provide important privacy protection. The legislation offers some protection against intrusion into seclusion and against the collection of some information, such as recordings of private conversations. 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.

---

1 *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 provision for the use of surveillance devices by federal law enforcement officers. However, it does not provide for offences applicable to general members of the public. 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: eg, s 21A(f) of the *Crimes Act 1958* (Vic).

2 *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices Act 1999* (Vic) pt 2A; *Workplace Privacy Act 2011* (ACT).

14.10 Protection from surveillance is a fundamental form of protection of privacy, particularly in the digital era. General Comment 16 of the UN Human Rights Committee specifically refers to surveillance, stating that:

> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.
>
> …
>
> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the [International Covenant on Civil and Political Rights].[3]

14.11 Sir Garfield Barwick, in the second reading speech for the Telephonic Communications (Interception) Bill 1960 (Cth), expressed a similar view:

> eavesdropping is abhorrent to us as a people. Not one of us, I am sure, would fail to recoil from the thought that a citizen's privacy could lightly be invaded. Indeed, many citizens no doubt feel that far too many intrusions into our privacy are permitted to be made in these times with complete impunity. Many things which might fairly be regarded as personal and of no public consequence appear in print without the citizen's permission and without his encouragement; but in particular all of us, I think, dislike the feeling that we may be overheard and that what we wish to say may reach ears for which we did not intend the expression of our thoughts. Much of our normal life depends on the confidence we can repose in those to whom we lay bare our sentiments and opinions, with and through whom we wish to communicate.[4]

14.12 As well as presenting a threat to privacy, surveillance threatens other important freedoms and liberties. Unauthorised surveillance may interfere with freedom of speech, freedom of movement and freedom of association. Professor Neil Richards identifies a chilling effect that surveillance may have on civil liberties:

> surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.[5]

14.13 Associate Professor Moira Paterson has described this chilling effect as occurring 'where people self adjust their behaviour even if they are not doing anything wrong':

---

3 Human Rights Committee, *General Comment No 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)*, 35th sess, UN Doc A/43/40 (28 September 1988) 16.

4 Commonwealth, *Parliamentary Debates*, House of Representatives, 5 May 1960 1 (Sir Garfield Barwick, Attorney-General).

5 Neil M Richards, 'The Dangers of Surveillance' [2013] *Harvard Law Review* 1934, 1935.

> The knowledge that their actions may be recorded and judged by unknown others may make individuals more self conscious about how they interact and what they say to other people, and even less willing to enter specific public places (for example, if they feel that they are not suitably dressed to be photographed or uncomfortable about others knowing that they frequent such places).[6]

14.14 Surveillance device laws protect individuals against invasions of privacy carried out through the use of various types of surveillance devices. The laws are therefore narrower in scope than the statutory tort set out in Part 2 of this Report. However, the possible consequences of a contravention of the surveillance device laws—conviction for a criminal offence—are potentially more significant than liability to pay damages for a serious invasion of privacy under the statutory tort.

A Commonwealth Act

Recommendation 14–1 The Commonwealth Government should enact surveillance legislation to replace existing state and territory surveillance device laws.

14.15 There are significant inconsistencies between existing state and territory surveillance device laws. There are differences between the laws with respect to the types of surveillance devices covered, the types of activities which amount to an offence, and the defences and exceptions that apply.

14.16 Existing surveillance device laws apply, variously, to 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.

14.17 The offences for carrying out surveillance are also inconsistent. For example:

- the offence for optical surveillance of a private activity in Victoria does not apply to activities carried on outside a building. This means that optical

6 Moira Paterson, 'Surveillance in Public Places and the Role of the Media: Achieving an Optimal Balance' (2009) 14 *Media and Arts Law Review* 241, 249.

surveillance of activities in a person's backyard, for example, is not an offence under the Victorian Act;[7]

- 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;[8] 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.[9]

14.18 There are also some significant differences between the defences and exceptions under existing surveillance device laws:

- some jurisdictions provide a 'participant monitoring' exception, allowing the surveillance of a private conversation or activity by a party to the conversation or activity, even if the other participants have not provided consent;[10]
- 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;[11]
- 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;[12]
- 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 recording, or a report of the recording, to anyone who was not a party to the conversation or activity;[13] and

---

7 *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.

8 *Surveillance Devices Act 2007* (NSW) ss 8, 10.

9 *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9.

10 *Invasion of Privacy Act 1971* (Qld) s 43(2)(a); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1); *Surveillance Devices Act* (NT) ss 11(1)(a), 12(1)(a).

11 *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); *Listening Devices Act 1992* (ACT) s 4(3)(a).

12 *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); *Listening Devices Act 1992* (ACT) s 4(3)(b)(i).

13 *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(ii); *Listening Devices Act 1991* (Tas) s 5(3)(b)(ii), (ACT) s 4(3)(b)(ii).

- some jurisdictions provide an exception where the use of a surveillance device is in the public interest.[14]

14.19 Due to these inconsistencies, the legal rights and interests of an individual who is under surveillance, and the legal liabilities of an individual or organisation that uses a surveillance device, are highly contingent upon their location.

14.20 Other inconsistencies exist with respect to issues such as the use of surveillance devices by law enforcement, the issuing of warrants, and cross-border investigations. These inconsistencies have been considered by the Standing Committee of Attorneys-General and the Australasian Police Ministers Council Working Group on National Investigation Powers.[15] This process resulted in the passage of the *Surveillance Device Act 2004* (Cth), which regulates the use of surveillance devices by federal law enforcement officers, but does not regulate the use of surveillance devices by individuals more generally.

14.21 There was widespread agreement from stakeholders about the desirability of surveillance device laws applying in the same way across Australia. Several stakeholders noted the benefits in protecting the privacy of individuals.[16]

14.22 Many stakeholders also noted the benefits to businesses, particularly where a business operates in multiple states or territories. The Australian Bankers' Association, for instance, submitted that:

> Banks and many other businesses operate on a national basis and are able to conduct their businesses more efficiently, with better convenience for their customers and in order to comply with consumer protection type laws if those laws are nationally uniform or consistent. National consistency contributes to national productivity and better outcomes for consumers.[17]

14.23 The Media and Communications Committee of the Law Council of Australia similarly submitted that:

> The Federal, State and territory laws governing surveillance devices, tracking devices, listening devices laws and unlawful surveillance are an inconsistent patchwork with no unifying principles of operation.
>
> This is an existing 'red tape' cost to business. National laws should operate in this area and those laws should be based upon a coherent rationale for regulation.[18]

---

14 *Surveillance Devices Act 1998* (WA) s 24 (definition of 'public interest'); *Surveillance Devices Act* (NT) s 41 (definition of 'public interest').

15 Standing Committee of Attorneys-General and the Australasian Police Ministers Council Working Group on National Investigation Power, *Cross-Border Investigative Powers for Law Enforcement*, Report (November 2003).

16 See, for example, Australian Privacy Foundation, *Submission 110*.

17 Australian Bankers' Association, *Submission 84*. See also Telstra, *Submission 107*; AMTACA, *Submission 101*.

18 Media and Communications Committee of the Law Council of Australia, *Submission 124*.

14.24 Free TV also noted the benefits for media organisations of having the same law throughout Australia,[19] while the Australian Institute of Professional Photography submitted that 'uniform Commonwealth laws are essential so that individual small photography businesses have some level of certainty about how they can operate anywhere in Australia'.[20]

14.25 While there was wide agreement on the need for removing inconsistencies, a number of stakeholders were concerned about the basis on which this might be achieved. The Australian Privacy Foundation, for example, submitted that

> uniformity should not be achieved at the expense of watering down Australians' rights to be free from unauthorised surveillance and any standardisation should be based on 'best practice' protection of privacy and not on 'lowest common denominator' protection.[21]

14.26 SBS supported uniformity, 'provided that the legislation allows for broad public interest concerns to permit both the creation of a recording, and the subsequent communication of that recording by the media'.[22]

14.27 The ALRC recommends that Commonwealth legislation should be introduced to cover the field with respect to surveillance devices. This legislation would effectively replace the existing state and territory surveillance device laws, and ensure that the law of surveillance devices was the same throughout Australia. Stakeholders were generally supportive of the introduction of federal legislation to cover the field of surveillance device law.[23]

14.28 Commonwealth surveillance devices legislation would likely be supported by 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.[24] The external affairs power allows the federal government to enact legislation that may be reasonably considered appropriate and adapted to fulfilling an obligation under an international treaty.[25] Since the primary purpose of surveillance legislation is the protection of privacy, it is likely that this requirement would be met.

14.29 Commonwealth legislation would likely be subject to some constitutional limitations with respect to state law enforcement agencies. The *Melbourne Corporation*

---

19 Free TV, *Submission 109*. Other media organisations expressing support for uniformity in surveillance device laws included SBS, *Submission 123*; ABC, *Submission 93*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

20 Australian Institute of Professional Photography (AIPP), *Submission 95*.

21 Australian Privacy Foundation, *Submission 110*.

22 SBS, *Submission 123*.

23 Australian Information Security Association (AISA), *Submission 117*; Australian Privacy Foundation, *Submission 110*; AMTACA, *Submission 101*; Australian Institute of Professional Photography (AIPP), *Submission 95*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; D Butler, *Submission 74*. However, the Office of the Victorian Privacy Commissioner stated a preference for states and territories retaining jurisdiction over surveillance devices: Office of the Victorian Privacy Commissioner, *Submission 108*.

24 The external affairs power and the ICCPR are discussed further in Ch 4.

25 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Victoria v Commonwealth* (1996) 187 CLR 416.

doctrine prevents the Commonwealth from enacting laws interfering with the capacity of the states to function as governments.[26] Due to this doctrine, it may be necessary for federal surveillance devices legislation to include provisions either exempting state law enforcement agencies from the federal surveillance devices legislation or providing a defence for surveillance carried out in accordance with a state law.

14.30 As an alternative to the Commonwealth enacting surveillance legislation to cover the field, states and territories could develop uniform or mirror surveillance legislation. However, some stakeholders expressed reservations about this approach. The Australian Privacy Foundation submitted that 'requiring agreement among the States and Territories is likely to lead to a protracted law reform process'.[27] Professor Des Butler noted that

> Near uniformity was achieved in defamation laws through the actions of [the Standing Committee of Attorneys-General], but only after over 20 years of debate. While the experience with defamation laws serves as an example where uniformity is possible, the position regarding surveillance devices would appear to reflect such disparate agendas among the jurisdictions that it may be preferable for the Commonwealth to legislate to cover the field in this instance.[28]

14.31 Given such concerns, the ALRC considers that it would be preferable for the Commonwealth Government to enact surveillance legislation which would apply in the same way throughout Australia.

Technology neutral surveillance legislation

Recommendation 14–2 Surveillance legislation should be technology neutral. It should regulate surveillance through the use of listening devices, optical devices, tracking devices, data surveillance devices, and other devices and systems.

14.32 The ALRC recommends that surveillance legislation be technology neutral. This would mean that surveillance legislation could more readily be applied to any existing or emerging technology that could be used for surveillance. The ALRC is not recommending particular technology neutral definitions. However, the ALRC considers that the surveillance legislation should apply, at least, to the types of devices recognised under existing laws: listening devices, optical surveillance devices, tracking devices and data surveillance devices. The legislation should also apply to technologies that may be considered to fall outside the ordinary meaning of 'device', such as software or networked systems.

14.33 The existing, technology-specific laws lead to inadequate protections from surveillance. For example:

---

26 *Melbourne v Commonwealth* (1947) 74 CLR 31; *Austin v Commonwealth* (2003) 215 CLR 185; *Clarke v Commissioner of Taxation* (2009) 240 CLR 272.

27 Australian Privacy Foundation, *Submission 110*.

28 D Butler, *Submission 74*.

- A whispered conversation in a public place may be a 'private conversation' and yet not a 'private activity', since the parties ought reasonably to expect to be observed, but ought reasonably expect not to be heard. Optical surveillance offences would therefore not apply, yet an optical recording of the conversation could be used in conjunction with lip-reading software to determine the words spoken.[29]
- An optical recording of someone's smart phone screen in a public place may not amount to surveillance of a private activity. It would also not amount to data surveillance, since the surveillance device laws that define 'data surveillance device' exclude optical surveillance devices from that definition.[30]
- Tracking the movements of an individual using their mobile phone does not amount to an offence under the *Surveillance Devices Act 1999* (Vic), since a 'tracking device' under that Act is 'an electronic device *the primary purpose of which* is to determine the geographical location of a person or an object'.[31] By excluding devices with tracking capabilities that are not a primary purpose—such as mobile phones—such a definition is limited in its application.

14.34 In addition to recognising existing types of surveillance devices, surveillance legislation should also recognise emerging technologies that may be used for carrying out surveillance. Four technologies, in particular, have generated some degree of community concern:

- unmanned aerial vehicles (drones) capable of being fitted with listening devices or optical surveillance devices;[32]
- wearable surveillance devices;[33]
- data surveillance devices in addition to those that can monitor information passing into or out of a computer system, such as radio frequency identification (RFID) readers;[34] and

---

29 A similar point was made by the Victorian Law Reform Commission in Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [6.11].

30 *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of 'data surveillance device'); *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'data surveillance device'); *Surveillance Devices Act* (NT) s 4 (definition of 'data surveillance device').

31 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'tracking device') (emphasis added).

32 At the time of writing, the House of Representatives Standing Committee on Social Policy and Legal Affairs was conducting an inquiry into the use of drones: 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). Several stakeholders expressed concerns about drones: 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*. The use of drones in farming contexts was a specific concern: Barristers' Animal Welfare Panel and Voiceless, *Submission 64*; National Farmers' Federation, *Submission 62*; RSPCA, *Submission 49*; Australian Lot Feeders' Association, *Submission 14*.

33 Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; D Butler, *Submission 10*; P Wragg, *Submission 4*.

34 M Paterson, *Submission 60*.

- tracking devices other than more traditional self-contained devices, such as networks that can locate an individual moving through an area over time.[35]

14.35 In many cases, these emerging technologies will fall within an existing definition. A drone fitted with an optical surveillance device, for example, will fall within the existing definitions of 'optical surveillance device', and a wearable microphone will fall within the existing definitions of 'listening device'. In other cases, however, a method of surveillance may not fall within any of the existing definitions. A technology neutral approach would avoid this limitation.

14.36 Submissions were generally supportive of a technology neutral approach to surveillance device laws.[36] For example, Free TV submitted that '[a] technologically neutral definition of "surveillance device" would further promote consistency across devices'.[37]

14.37 However, some stakeholders expressed concerns that technology neutral legislation may fail to capture important distinctions between different types of devices. The Australian Privacy Foundation submitted that

> there may well be particular technologies which give rise to specific concerns. Where this is the case, or where it is necessary to avoid doubt about whether or not a type of device is subject to the law, there may be an inescapable need for definitions to refer to particular technologies.[38]

14.38 Similarly, the UNSW Cyberspace Law and Policy Community agreed that

> The 'technology neutral' idea for surveillance device is a good one in principle, but also needs to distinguish between very different technologies, eg drones with cameras and data surveillance by software, to the extent they raise different issues. In practice such neutrality is difficult to achieve, and may omit or overlook some of the potential for new or divergent technology to raise particular issues not considered previously.[39]

14.39 On balance, the ALRC considers that the benefits of a technology neutral approach outweigh the risks. Moreover, the risks can be reduced through appropriate framing of other legislative provisions. First, certain types of devices, such as the four types falling within the existing definitions, could be explicitly defined as surveillance devices. This would help to ensure that such devices did not fall outside the scope of surveillance legislation. Secondly, many of the distinctions between different types of devices can be adequately reflected in the surveillance offences themselves. The ALRC agrees, for example, that optical surveillance devices and data surveillance devices may raise different issues and lend themselves to different forms of surveillance. However, these differences can be adequately reflected in offences that distinguish between, for

---

35 Ibid; Electronic Frontiers Australia, *Submission 44*.

36 Australian Information Security Association (AISA), *Submission 117*; T Butler, *Submission 114*; Office of the Victorian Privacy Commissioner, *Submission 108*; Telstra, *Submission 107*; Australian Sex Party, *Submission 92*; Australian Bankers' Association, *Submission 84*; Australian Pork Ltd, *Submission 83*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; Women's Legal Services NSW, *Submission 76*; D Butler, *Submission 74*.

37 Free TV, *Submission 109*.

38 Australian Privacy Foundation, *Submission 110*.

39 UNSW Cyberspace Law and Policy Community, *Submission 98*.

example, recording a private activity (which might be carried out with an optical surveillance device) and monitoring the information entered into an information system (which might be carried out with a data surveillance device). The ALRC considers it undesirable to restrict offences to surveillance carried out using particular devices, as is the case under existing laws.

14.40 The Australian Institute of Professional Photography expressed a concern that a technology neutral definition may be overly broad:

> 'surveillance' and 'surveillance devices' need to be defined with great precision, so that a commercial photographer is not prevented merely from capturing activity in public.[40]

14.41 Technology neutral legislation may be broad in scope and may capture many devices that can be used for legitimate purposes, such as cameras. However, although a broad range of devices may be captured by technology neutral laws, an offence would only be made out where the particular use of the device is inappropriate. Existing surveillance device laws require various conditions to be met for an offence to be made out. For example, under the *Surveillance Devices Act 1998* (WA), optical surveillance is only an offence where it involves recording or observing a 'private activity' defined as:

> any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed.[41]

14.42 Under this definition, an activity carried on in public would generally not be a 'private activity', to the extent that the parties ought reasonably to expect that the activity may be observed. Such a definition would clearly exclude activities taking place, for example, in public streets, on public beaches, or at public events. It would not be sufficient that the activity was of a private, personal or intimate nature.

Telecommunications surveillance

Recommendation 14–3 The Commonwealth Government should consider consolidating telecommunications surveillance laws with the new Commonwealth surveillance legislation.

14.43 The ALRC recommends that, if the Commonwealth enacts surveillance legislation, consideration be given to integrating surveillance device laws with the related restrictions on telecommunications surveillance under the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act).

---

40 Australian Institute of Professional Photography (AIPP), *Submission 95*. Several stakeholders expressed related concerns that surveillance legislation may make unlawful the legitimate activities of film makers, photographers, and other artists whose work involves surveillance devices: Arts Law Centre of Australia, *Submission 113*; National Association for the Visual Arts Ltd, *Submission 78*.

41 *Surveillance Devices Act 1998* (WA) s 3(1) (definition of 'private activity').

14.44 The existing surveillance device laws do not regulate or address the entire range of activities that might be thought of as 'surveillance'. In particular, the surveillance device laws do not regulate surveillance of telecommunications systems. Australian law recognises a distinction between, on the one hand, surveillance carried out using devices such as cameras or listening devices and, on the other hand, surveillance carried out through the interception of communications. The use of the latter type of surveillance is primarily regulated under the TIA Act. Collection and surveillance of communications data ('metadata') is also regulated by the TIA Act.

14.45 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.[42] Thus, while a tape recorder placed next to the speaker of a telephone handset to record a private telephone conversation would engage a surveillance device law, unauthorised interception of that private telephone conversation would engage the TIA Act.

14.46 The distinction between interception and surveillance is likely to become increasingly artificial as the convergence of computer systems and telecommunications systems increases. This may result in some surveillance activities being over-regulated, while other surveillance activities fall outside the scope of either regulatory regime. There may therefore be merit in integrating a federal surveillance device law with federal law regulating surveillance of telecommunications systems. Such integration may provide increased certainty to individuals, and may have the additional benefit of reducing the complexity of these laws for businesses and organisations that must deal with them.

14.47 However, in considering any integration of these laws, it would be important to ensure that privacy protections of individuals were not weakened, that compliance burdens on businesses and organisations were not increased, and that appropriate oversight and monitoring mechanisms were put in place applying to all forms of surveillance. Differences between different types of surveillance would also need to be considered. For example, while surveillance with a listening device may involve an intention on the part of the person carrying out the surveillance to record the conversation of a specific individual, telecommunications surveillance may involve the collection or processing of data about many individuals simultaneously. On the other hand, special defences or exceptions may be required for surveillance-like activities—such as the determination of individuals' locations—that may be technologically necessary for the proper operation of telecommunications networks.

Participant monitoring

Recommendation 14–4 Surveillance legislation should not contain a defence or exception for participant monitoring.

42 *Miller v Miller* (1978) 141 CLR 269.

14.48 Existing state and territory surveillance laws differ as to whether a party to a private conversation or activity may record that conversation or activity without the consent of the other participants. Such recording is referred to as 'participant monitoring'. The surveillance device laws of Queensland, Victoria and the Northern Territory contain participant monitoring exceptions.[43] The surveillance device laws in the remaining jurisdictions do not contain such exceptions. This is a significant divergence in the protection of individuals' privacy across Australia.

14.49 The ALRC considers that surveillance legislation should not contain defences or exceptions for participant monitoring. The protections offered by surveillance device laws are significantly undermined if a party to a private activity (including a private conversation) may record the activity without the knowledge or consent of other parties. Where individuals take part in an activity under the reasonable belief that the activity is private, their privacy should not be undermined by covert surveillance by other parties to that activity. If individuals cannot enter such activities secure in the assumption that they will not be placed under surveillance by other parties, there may be a chilling effect that discourages individuals from taking part in some private activities and from speaking freely in private conversations. This is an increasing risk given the readily-available consumer technologies that allow for surreptitious recording.

14.50 A number of stakeholders supported the removal of participant monitoring exceptions.[44]

14.51 This recommendation is consistent with recommendations made by other law reform inquiries. The Victorian Law Reform Commission in its 2009 report on surveillance also recommended the removal of the participant monitoring exception from the *Surveillance Devices Act 1999* (Vic):

> It 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. Without this knowledge, those people cannot refuse to be recorded or alter their behaviour. These concerns apply even more strongly in the case of activities or conduct in private places.[45]

14.52 The NSW Law Reform Commission (NSWLRC) considered, and ultimately rejected, a participant monitoring exception in its 1998 interim report on surveillance.[46]

14.53 The ALRC's recommendation is consistent with the approach under the TIA Act, which, along with the surveillance device laws, is the primary regulation of surveillance activities in Australia. Under s 7 of the TIA Act, the offence of intercepting telecommunications does not include a participant monitoring exception.

---

43 *Invasion of Privacy Act 1971* (Qld) s 43(2)(a); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1); *Surveillance Devices Act* (NT) ss 11(1)(a), 12(1)(a).

44 Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

45 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [6.57], rec 18.

46 NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) rec 14, [2.99]–[2.107].

14.54 Several stakeholders suggested that surveillance legislation should contain a participant monitoring exception, and that the focus should instead be on restricting the disclosure of information obtained through surveillance. For example, the ABC submitted that:

> it is arguable that the recording by a participant is not the problem and that it is the further communication of the recorded private activity which should be proscribed, subject to relevant defences.[47]

14.55 It may be possible to develop a model of surveillance regulation based on restricting communication of information obtained through surveillance, rather than restricting the surveillance itself. On balance, however, the ALRC considers that it is preferable to regulate the act of surveillance itself. Surveillance, even without further communication of the information obtained, may in itself cause harm to the individuals under surveillance. The New Zealand Law Commission, for example, identified a range of harms that surveillance may cause an individual, regardless of whether the information obtained through the surveillance is communicated further. These harms include:

- a chilling effect on the exercise of civil liberties;
- loss of anonymity;
- stress and emotional harm;
- insecurity and loss of trust;
- use for voyeuristic or other questionable purposes;
- discrimination and misidentification; and
- desensitisation to surveillance, leading to a narrowing of people's reasonable expectations of privacy.[48]

14.56 There may be cases where participant monitoring of a private activity, without the knowledge or consent of other parties, is justifiable. In particular, surveillance without the consent of other parties may be justified where it is reasonably necessary for the protection of the lawful interests of the person conducting the surveillance or where it is for the purposes of recording a threat or abuse.[49]

14.57 The ALRC considers that these cases are more appropriately addressed through specific defences or exceptions, rather than through a general participant monitoring exception. Many such defences and exceptions are provided under existing surveillance device laws. A participant monitoring exception would allow surveillance even in

---

47 ABC, *Submission 93*.

48 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Report 113* (2010) 11; New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3*, Issues Paper No 14 (2009) 201–204.

49 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; J Chard, *Submission 88*.

cases where surveillance was not being used for the protection of lawful interests or for recording a threat or abuse.

Responsible journalism and the public interest

Recommendation 14–5 Surveillance legislation should provide a defence for responsible journalism relating to matters of public concern and importance.

14.58 Surveillance will sometimes be necessary and justified when conducted in the course of responsible journalistic activities. The ALRC recommends that surveillance legislation include a defence for responsible journalism, particularly if participant monitoring exceptions are not included in surveillance legislation. Media and journalistic activities offer significant public benefit, and these activities may at times justify the use of surveillance devices without the notice or consent of the individuals placed under surveillance. The removal of participant monitoring exceptions, as recommended above, would restrict the ability of journalists to use surveillance devices in this way.

14.59 For example, a journalist who records a private conversation in which a public figure is expected to reveal evidence of corruption would, absent a participant monitoring exception or other defence, have committed an offence under surveillance legislation. The ALRC considers that this is, generally speaking, an undesirable outcome that could be avoided through the introduction of a defence of responsible journalism.

14.60 At the same time, the ALRC considers that a defence of responsible journalism should be suitably constrained. The defence should not, for example, allow unrestricted freedom to carry out surveillance in circumstances which are not journalistic in nature, where the public interest in a matter is trivial, or where the matter is merely of interest to the public or for the purposes of gossip.

14.61 Consideration should be given to providing distinct responsible journalism defences for the distinct offences of, first, the installation or use of a surveillance device, and second, the communication of information obtained through surveillance. The circumstances that justify communication of information obtained through surveillance may be different from those that justify the installation or use of a surveillance device. A journalist is unlikely to know what information will be obtained under surveillance before the surveillance is completed—for example, a public official may or may not make a comment that suggests corruption during a particular recording.

14.62 A responsible journalism defence to the installation or use of a surveillance device should therefore depend whether it was reasonable for the journalist to believe that the use of the surveillance device was in the public interest, and not on whether the information obtained through surveillance was, in hindsight, information in the public interest. However, considerations of whether the information obtained was in the public interest may be relevant if a responsible journalism defence is to be applied to

the use or communication of information obtained through surveillance, rather than the act of surveillance itself.

14.63 The proposed defence of responsible journalism was supported by several stakeholders, although some stakeholders noted that the nature of the defence required further discussion and detail.[50] The Australian Privacy Foundation submitted that 'care would need to be exercised in defining who was entitled to an exception, as well as precisely limiting the circumstances in which surveillance might be permissible' and noted 'the potential for existing and emerging technologies to allow for widespread surveillance as part of 'fishing expeditions'.[51]

14.64 The ALRC is not recommending specific elements of such a defence, and further consideration would be required before such a defence was drafted. However some possible elements, drawn from other laws, include:

- the surveillance should be carried out for the purposes of investigating matters of significant public concern, such as corruption;
- the defendant must have reasonably believed that conducting the surveillance was in the public interest;[52]
- the surveillance was necessary and appropriate for achieving that public interest, and the public interest could not have been satisfied through other reasonable means; and
- the defendant must have been an employee or member of an organisation that had publicly committed to observing standards dealing adequately with the appropriate use of surveillance devices by media and journalists.[53]

14.65 Historically, 'responsible journalism' was developed as a defence to defamation in *Reynolds v Times Newspapers Ltd*.[54] Despite being crafted in the context of defamation, several of the matters listed by Nicholls LJ are relevant in the context of surveillance. For example, the seriousness of the conduct being investigated by a journalist, the likely strength of the individual under surveillance as a source of information, the likely nature of the information obtained, and the urgency of the matter may be relevant considerations.[55]

14.66 The *Reynolds* defence was considered further in *Jameel (Mohammed) v Wall Street Journal Europe Sprl*.[56] There, Lord Hoffman observed that

---

50 Office of the Victorian Privacy Commissioner, *Submission 108*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.

51 Australian Privacy Foundation, *Submission 110*.

52 See, for example, s 4 of the *Defamation Act 2013* (UK), discussed below.

53 A similar requirement can be found in the media exemption under the *Privacy Act*: *Privacy Act 1988* (Cth) s 7B(4); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 42–3.

54 *Reynolds v Times Newspapers Ltd* [2001] 2 AC 127.

55 Ibid 205 (Nicholls LJ).

56 *Jameel (Mohammed) v Wall Street Journal Europe Sprl* [2006] UKHL 44.

> opinions may reasonably differ over which details are needed to convey the general message. The fact that the judge, with the advantage of leisure and hindsight, might have made a different editorial decision should not destroy the defence. That would make the publication of articles which are, *ex hypothesi*, in the public interest, too risky and would discourage investigative reporting.[57]

14.67 The *Reynolds* defence to defamation was abolished and replaced by s 4 of the *Defamation Act 2013* (UK). That section provides:

> 4 Publication on matter of public interest
>
> (1) It is a defence to an action for defamation for the defendant to show that—
>
> (a) the statement complained of was, or formed part of, a statement on a matter of public interest; and
>
> (b) the defendant reasonably believed that publishing the statement complained of was in the public interest.
>
> …
>
> (4) In determining whether it was reasonable for the defendant to believe that publishing the statement complained of was in the public interest, the court must make such allowance for editorial judgement as it considers appropriate.

14.68 Media policies also provide some guidance on where the use of surveillance by media or journalists may be appropriate in the public interest. In its submission to the Issues Paper, the ABC noted clause 5.8 of its editorial policy, which provides guidance on the use of surveillance by ABC journalists:

> Secret recording and other types of deception
>
> 5.8 Secret recording devices, misrepresentation or other types of deception must not be used to obtain or seek information, audio, pictures or an agreement to participate except where:
>
> a justified in the public interest and the material cannot reasonably be obtained by any other means; or
>
> b consent is obtained from the subject or identities are effectively obscured; or
>
> c the deception is integral to an artistic work and the potential for harm is taken into consideration.

14.69 Clause 5.8(a), in particular, requires that the recording must not only be in the public interest but must be the only reasonable way to obtain the material.

14.70 An alternative to a specific defence of responsible journalism is a defence of public interest. Such a defence would be broader than a responsible journalism defence, and the limits of such a defence would need to be clearly circumscribed.

14.71 Several existing surveillance device laws include exceptions to offences where surveillance is carried out in the public interest. Under the *Surveillance Devices Act 1999* (Vic), the offence for communicating information obtained through surveillance does not apply 'to a communication or publication that is no more than is reasonably

---

57 Ibid [51] (Lord Hoffmann).

necessary … in the public interest'.[58] The *Listening and Surveillance Devices Act 1972* (SA) permits the use of a listening device by a party to a private conversation if the use is in public interest,[59] and permits the communication of information obtained through surveillance in the public interest.[60]

14.72 The *Surveillance Devices Act 1998* (WA) and the *Surveillance Devices Act* (NT) each allow for emergency use of surveillance devices in the public interest,[61] and each define 'public interest' to include 'the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens'.[62]

14.73 Section 31 of the *Surveillance Devices Act 1998* (WA) allows a judge to make an order allowing information obtained through surveillance to be published. Such an order requires that a person make an application for such an order and that 'the judge is satisfied … that the publication or communication should be made to protect or further the public interest'. However, such applications have met with 'mixed success'.[63]

14.74 In *Channel Seven Perth v 'S' (A Company)*,[64] Channel Seven Perth appealed against a decision dismissing its application for an order under s 31 of the *Surveillance Devices Act 1998* (WA). Channel Seven had asked a woman ('M') to secretly record a meeting with her manager about her dismissal due to pregnancy, and sought an order allowing broadcast of the recording. The Western Australian Court of Appeal dismissed the appeal, finding that:

- there was public interest in the matter, relating to equal opportunity and unfair dismissal;
- the circumstances of the recording indicated that the meeting between M and her manager was a private conversation and a private activity;
- the manager's purpose in explaining the reasons for M's dismissal was to be encouraged, and the possibility of that explanation being recorded would act as a disincentive;
- the same public interest issues could have been raised without the use of surveillance, notwithstanding that a recording may 'more effectively stimulate audience interest in the issues';[65] and

58 *Surveillance Devices Act 1999* (Vic) s 11(2)(b).
59 *Listening and Surveillance Devices Act 1972* (SA) s 7(1).
60 Ibid s 7(3)(c).
61 *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), part 5; *Surveillance Devices Act* (NT) ss 11(2)(c), 12(2)(d), 43, 44.
62 *Surveillance Devices Act 1998* (WA) s 24 (definition of 'public interest'); *Surveillance Devices Act* (NT) s 41 (definition of 'public interest').
63 David Rolph, Matt Vitins and Judith Bannister, *Media Law: Cases, Materials and Commentary* (Oxford University Press, 2010) 646.
64 *Channel Seven Perth Pty Ltd v 'S' (A Company)* [2007] WASCA 122.
65 Ibid [40] (McClure JA).

- if the matters relied on by Channel Seven Perth were sufficient to meet the public interest test of s 31, there could be 'widespread use by the media of covertly obtained private information',[66] inconsistent with the language and purpose of the *Surveillance Devices Act 1998* (WA).

14.75 The decision in *Channel Seven Perth v 'S' (A Company)* recognises that surveillance may not be the only way that a particular public interest goal could be achieved. It may be appropriate for a defence of responsible journalism to apply only where the surveillance was necessary.

14.76 The ALRC considers that a more restricted responsible journalism defence is preferable to a broader public interest defence. Journalists and media groups will typically have standards in place, such as the editorial policy of the ABC referred to above, and compliance with such a standard may be an important limitation of the defence. Furthermore, a broader public interest test may allow for wider use of surveillance, with defendants attempting to justify their use of surveillance devices based on their own subjective views about what is in the public interest.

Workplace surveillance

Recommendation 14–6 Workplace surveillance laws should be made uniform throughout Australia.

14.77 Workplace surveillance legislation is 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.

14.78 The ALRC received few submissions discussing workplace surveillance laws. The recommendations in this chapter therefore focus on the more general surveillance device laws. However, stakeholders who did refer to workplace surveillance laws supported uniformity in those laws.[67]

14.79 Specific workplace surveillance laws (the workplace surveillance laws) exist only in NSW,[68] the ACT[69] and, to some extent, in Victoria.[70] As with general surveillance device laws, uniformity in workplace surveillance laws would promote certainty, particularly for employers and employees located in multiple jurisdictions.

14.80 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

66 Ibid.
67 Pirate Party of Australia, *Submission 119*; Australian Privacy Foundation, *Submission 110*; Redfern Legal Centre, *Submission 94*; Guardian News and Media Limited and Guardian Australia, *Submission 80*.
68 *Workplace Surveillance Act 2005* (NSW).
69 *Workplace Privacy Act 2011* (ACT).
70 *Surveillance Devices Act 1999* (Vic) pt 2A.

activities of workers in workplace toilets, washrooms, change rooms or lactation rooms.[71] Workplace surveillance in Victoria is otherwise subject to the same restrictions as general surveillance devices.

14.81 The *Workplace Privacy Act 2011* (ACT) applies to optical devices, tracking devices and data surveillance devices, but not to listening devices.[72] 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.[73] 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.[74] The ACT Act also prohibits 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.[75]

14.82 The *Workplace Surveillance Act 2005* (NSW) similarly applies only to 'optical surveillance', 'computer surveillance' and 'tracking surveillance'.[76] The NSW Act contains similar restrictions to those in the ACT. Surveillance devices must not be used in a workplace without sufficient notice being provided to employees,[77] must not be used in a change room, toilet, or shower facility,[78] and must not be used to conduct surveillance of the employee outside work.[79] Covert surveillance must not be used unless a covert surveillance authority is obtained.[80] The NSW Act also places limitations on the restriction of employee email and internet access while at work.[81]

14.83 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 three jurisdictions. The ALRC therefore recommends that there be uniform workplace surveillance laws across Australia.

---

71 Ibid s 9B.
72 *Workplace Privacy Act 2011* (ACT) s 11(1) (definition of 'surveillance device').
73 Ibid pt 3.
74 Ibid pt 4.
75 Ibid pt 5.
76 *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.
77 Ibid pt 2.
78 Ibid s 15.
79 Ibid s 16. An exception applies where the surveillance is computer surveillance on equipment provided at the employer's expense.
80 Ibid pt 4.
81 Ibid s 17.

14.84 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.[82]

Remedial relief and compensation

Recommendation 14–7 Surveillance legislation should provide that a court may order remedial relief, including compensation, for a person subjected to unlawful surveillance.

14.85 The ALRC recommends that surveillance legislation allow a court to make a compensation order or provide remedial relief to an individual who has been the subject of unlawful surveillance. This proposal was supported by several stakeholders.[83]

14.86 A similar mechanism for compensation can be found in s 107A of the *Telecommunications (Interception and Access) Act* 1979 (Cth) (the TIA Act). 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.[84] If surveillance legislation were enacted by the Commonwealth, there would be merit in both surveillance legislation and the TIA Act providing similar options for compensation and redress.

14.87 Criminal law generally punishes the offender without necessarily providing redress to the 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 and others from conducting further unlawful surveillance in the future, the victim will generally not receive any compensation or other personal remedy.

14.88 Guardian News and Media Limited and Guardian Australia did not support this proposal, arguing that a tort for serious invasions of privacy would be the more appropriate mechanism for a victim of surveillance to obtain compensation.[85] However, in order to obtain compensation in this way, the individual would be required

---

82 The latter, integrated approach was recommended by the NSWLRC: NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) rec 57.

83 T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; D Butler, *Submission 10*.

84 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).

85 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

to undertake civil proceedings in addition to seeking a prosecution under surveillance legislation. The ALRC recommendation would provide a quicker, cheaper and easier means of redress where an offence has occurred.

14.89 All states and territories have established victims' compensation schemes that provide for compensation to be paid to victims of crimes.[86] Unlike an order for compensation to be paid by an offender, a victims' compensation scheme does not depend on an offender's ability for compensation to be paid. However, victims' compensation schemes are generally only available for serious physical crimes such as assault, robbery, or sexual assault,[87] and surveillance is therefore unlikely to give rise to compensation under these schemes.

Alternative forums for complaints about surveillance

> **Recommendation 14–8** State and territory governments should give jurisdiction to appropriate courts and tribunals to hear complaints about the installation and use of surveillance devices that can monitor neighbours on residential property.

14.90 The ALRC recommends that jurisdiction be conferred on appropriate courts and tribunals to allow residential neighbours' disputes about the use of surveillance devices to be heard by appropriate courts and tribunals. A number of submissions to this Inquiry have raised concerns regarding CCTV cameras, installed for security in homes and offices that may also record the activities of neighbours. A low cost option for resolving disputes about surveillance devices is desirable, particularly where prosecution under surveillance legislation is inappropriate, undesirable or unsuccessful. While such a dispute might also be settled by one neighbour seeking an injunction against the other under the law of nuisance, as in *Raciti v Hughes*,[88] such a process involves proceedings in superior courts. It would be desirable for a lower cost forum to be made available.

14.91 Courts and tribunals—such as the ACT Civil and Administrative Tribunal (ACAT); the NSW Land and Environment Court (LEC); the Queensland Planning and Environment Court (QPEC); the State Administrative Tribunal of Western Australia (SAT); and the Victorian Civil and Administrative Tribunal (VCAT)—have

86 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. The ABC noted the existence of these schemes in its submission to the Discussion Paper: ABC, *Submission 93*.

87 *Victims Rights and Support Act 2013* (NSW) s 5; *Victims of Crime Assistance Act 1996* (Vic) ss 7–13.

88 *Raciti v Hughes* (1995) 7 BPR 14, 837. The plaintiffs in this case successfully obtained an injunction to prevent the use of motion-triggered lights and surveillance cameras aimed at their backyard.

jurisdiction to hear a wide range of civil disputes and disputes relating to planning and development,[89] as well as disputes between neighbours.[90]

14.92 Many of the types of disputes that may currently be heard in these tribunals involve an element of privacy, and in particular the protection of privacy in disputes between neighbours. For example, in *Walnut Tree Development v Hepburn SC*[91] the VCAT required that additional fencing be included in a development plan in order to enhance the privacy of a neighbouring building. In *Des Forges v Kangaroo Point Residents Association*, the QPEC set aside development approval for three residential towers because 'insufficient regard has been paid to the actual intensity of the development, to boundary clearances, separation, privacy and the consequential effects on views'.[92] In *Meriton v Sydney City Council*,[93] the NSW LEC found that a building proposal would not have an unacceptable impact on privacy because of the particular angle of its windows. In *Szann v Council of the City of Sydney*,[94] the NSW LEC dismissed an appeal against a council decision rejecting the use of two security cameras with the ability to pan and zoom, noting that a fixed lens camera would have provided adequate surveillance. In *Szann*, the Court observed that:

> The presence of the dome camera, high on the rear elevation immediately adjacent to the shared boundary, is a menacing panoptic mechanism, positioned to give the neighbours the impression of being constantly observed in their own, private rear courtyard. Any camera, where the lens is visible from an adjoining property or the public domain, gives the perception that you are under surveillance, regardless of whether 'privacy masks' are enabled to veil unwanted zones, because you cannot see whether a privacy mask is enabled by looking at the camera. The barrel camera body of the fixed lens camera provides an assurance than when you are not in front of the cone view of the lens, you are not under surveillance.[95]

14.93 In the Discussion Paper, the ALRC asked whether local councils should be empowered to regulate the installation and use of surveillance devices by private individuals. Stakeholders were generally not supportive of local councils holding such a power. Concerns expressed in submissions included:

- inconsistency and fragmentation of surveillance laws;[96]
- weakening of 'strong national standards' of surveillance device regulation;[97]

---

89 The *South Australian Civil and Administrative Tribunal Act 2013* (SA) provides for the establishment of the South Australian Civil and Administrative Tribunal (SACAT). However, at the time of writing, the SACAT has not begun operation.

90 See, for example, the *Trees (Disputes Between Neighbours) Act 2006* (NSW). Many lower courts have jurisdiction over fencing disputes: see, eg, *Fences Act 1975* (SA).

91 *Walnut Tree Development Pty Ltd v Hepburn SC* [2003] VCAT 1271 (16 September 2003).

92 *Des Forges v Kangaroo Point Residents Association* [2001] QPEC 61 (21 September 2001) [213].

93 *Meriton v Sydney City Council* [2004] NSWLEC 313.

94 *Szann v Council of City of Sydney* [2012] NSWLEC 1168 (21 June 2012).

95 Ibid [32].

96 Arts Law Centre of Australia, *Submission 113*; Office of the Victorian Privacy Commissioner, *Submission 108*; T Hobson, *Submission 85*.

97 Australian Privacy Foundation, *Submission 110*.

- a risk of over-regulation, such as restrictions placed on photography during public events at public beaches;[98] and
- the limited experience of local council officers in regulating surveillance.[99]

14.94 Noting these concerns about the regulation of surveillance devices by local councils, the ALRC considers that there remains a benefit in having complaints about certain types of surveillance dealt with in forums that may provide resolution with less cost, less time, and less impact on parties.

14.95 The ALRC also considers that the resolution of neighbourhood disputes about surveillance device in courts and tribunals would avoid the concerns expressed by stakeholders about local council regulation:

- courts and tribunals operate at the state and territory level, ensuring consistency at that level—these powers would not be to the exclusion of the Commonwealth surveillance legislation;
- over-regulation of the type envisaged by stakeholders would be limited, since the powers would be limited to residential neighbour disputes and provided for under legislation; and
- courts and tribunals have existing experience in dealing with privacy issues in the context of neighbour disputes.

98 Australian Institute of Professional Photography (AIPP), *Submission 95*.

99 Arts Law Centre of Australia, *Submission 113*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; National Association for the Visual Arts Ltd, *Submission 78*.

15. Harassment

Contents

Summary 299
Statutory tort of harassment 300
Existing civil remedies 301
A harassment tort 302
Uniform state and territory legislation 303
Criminal offences for harassment 304
State stalking and harassment laws 304
Commonwealth cyber-harassment laws 305
Harassment laws in other countries 307

Summary

15.1 Many serious invasions of privacy also amount to harassment. Harassment involves a pattern of behaviour or a course of conduct pursued by an individual with the intention of intimidating and distressing another person. Harassment often involves intruding into someone's private space and affairs, and perhaps misusing their personal information. Laws that target harassment will therefore often also serve to protect people's privacy.

15.2 In this chapter, the ALRC recommends that if a privacy tort is not enacted, the states and territories should enact a statutory tort of harassment, to provide those subjected to harassment with a means of civil redress.

15.3 Harassment legislation would provide Australians with protection similar to that in other countries, including the United Kingdom, New Zealand and Singapore.

15.4 Further consideration of the detailed design of a harassment tort will be necessary. Generally, a new harassment tort should capture a course of conduct that is genuinely oppressive and vexatious, not merely irritating or annoying. The tort should be confined to conduct that is intentionally designed to harm or demean another individual.

15.5 A harassment tort should also be the same throughout the country. The states and territories should therefore enact uniform legislation, if the Commonwealth does not have the Constitutional power to enact a harassment tort.

15.6 This chapter also highlights some gaps and inconsistencies in existing criminal laws concerning harassment, as well as some challenges for their enforcement.

Statutory tort of harassment

Recommendation 15–1 If a statutory cause of action for serious invasion of privacy is not enacted, state and territory governments should enact uniform legislation creating a tort of harassment.

15.7 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.

15.8 In some instances, harassment will clearly amount to an interference with someone's privacy. For example, the following conduct—where it is repeated, unwanted and intended to distress and demean an individual—may amount to harassment and an invasion of privacy:

- following or keeping someone under surveillance;
- eavesdropping and wiretapping;
- reading private letters and other private communication;[1]
- using surveillance devices to monitor, intimidate or distress someone;[2]
- publishing private information;
- taking photos of someone in a private context, without their permission; and
- making persistent and unwanted contact, such as by telephone or email.[3]

15.9 The ALRC has received submissions from numerous stakeholders outlining different forms of behaviour that would seem to amount to both harassment and a serious invasion of privacy.[4]

15.10 If a new tort for serious invasions of privacy is not enacted, the ALRC recommends the enactment of a statutory cause of 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.

---

1 Ruth Gavison, 'Privacy and the Limits of the Law' (1979) 89 *Yale Law Journal* 421, 429.

2 In *Howlett v Holding*, an injunction was granted 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: *Howlett v Holding* [2006] EWHC 41 (QB) (25 January 2006).

3 Some of these are examples of conduct that has been the subject of claims under the *Protection from Harassment Act 1997* (UK).

4 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Women's Legal Services NSW, *Submission 115*; National Children and Youth Law Centre, *Submission 61*; Women's Legal Service Victoria and Domestic Violence Resource Centre Victoria, *Submission 48*.

Existing civil remedies

15.11 There are gaps and limitations in existing civil remedies for persons subjected to harassment.

15.12 Australian courts 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',[5] citing the work of Professor Stephen Todd from New Zealand.[6] New Zealand has now enacted the *Harassment Act 1997* (NZ) and the courts have recognised a tort of intrusion into seclusion.[7]

15.13 In *Grosse v Purvis*,[8] 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.

15.14 At present, Australian law does not provide civil redress to the victims of harassment. There is some protection in defamation law, as well as the torts of battery or trespass to the person where conduct becomes physically threatening or harmful. If bullying or harassment, including cyber-bullying, occurs on school property within school hours, a school may be liable under the law of negligence on the basis of a non-delegable duty of care.[9]

15.15 However, 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 in the common law.[10] For example, the tort of trespass to land can be used only where there has been an unlawful intrusion onto property.[11] 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.[12]

15.16 Harassment may not involve any physical contact amounting to battery, or threat of physical contact amounting to assault.[13]

---

5 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [123].

6 Stephen Todd, 'Protection of Privacy' in Nicholas Mullany (ed), *Torts in the Nineties* (LBC Information Services, 6th ed, 1997).

7 *C v Holland* [2012] 3 NZLR 672. The New Zealand provision is discussed further below.

8 *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.

9 *Commonwealth v Introvigne* (1982) 150 CLR 258.

10 See Barbara McDonald, 'Tort's Role in Protecting Privacy: Current and Future Directions' in J Edelman, J Goudkamp and S Degeling (eds), *Torts in Commercial Law* (Thomson Reuters, 2011).

11 *Plenty v Dillon* (1991) 171 CLR 635.

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

13 Rosalie Balkin and Jim Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [3.16].

15.17 The tort of nuisance requires an interference with the lawful occupier's use and enjoyment of land.[14] Nuisance has been useful in limited cases, such as where a CCTV camera was erected at a neighbour's backyard, prohibiting their use and enjoyment of the garden.[15] However, again, a person's right to sue is limited.[16]

15.18 The tort of wilful infliction of nervous shock[17] is an inadequate remedy for many instances of harassment, as a plaintiff must prove actual physical or psychiatric injury. Harassment, however, will often result only in emotional distress.

A harassment tort

15.19 Given these gaps, the ALRC recommends the enactment of a new tort to provide civil remedies, including damages, to persons subjected to harassment. Several stakeholders supported a statutory tort of harassment.[18] The tort would be actionable where there is a course of conduct, linked by a common purpose and subject-matter, intentionally committed to cause distress and intimidation. Further work is necessary on the detailed design of the tort, but these might be the key elements.

15.20 It is important that the threshold is not set too low, so the new tort does not capture behaviour which is merely irritating or slightly disturbing. A new tort for harassment would provide for a targeted avenue of civil redress where the conduct is not redressed by existing torts. Civil remedies, particularly compensatory damages, can vindicate a plaintiff's interests.[19]

15.21 Several stakeholders opposed the introduction of a statutory tort of harassment.[20] For example, the Australian Mobile Telecommunications Association and Communications Alliance argued that the existing privacy regulatory framework is adequate to prevent and redress conduct amounting to harassment.[21] However, the ALRC considers the gaps identified above demonstrate the need for a civil action in privacy or harassment.

15.22 Guardian News and Media Limited and Guardian Australia submitted that it would be preferable to introduce the new privacy tort than modify existing laws relating to harassment.[22] Their submission raises the concern that a harassment tort does not involve a public interest balancing test, unlike the new privacy tort. Given

---

14 Ibid [14.1].
15 *Raciti v Hughes* (1995) 7 BPR 14, 837.
16 *Hunter and Others v Canary Wharf Ltd; Hunter and Others v London Docklands Corporation* [1997] UKHL 14.
17 *Wilkinson v Downton* (1897) 2 QB 57; *Nationwide News Pty Ltd v Naidu* (2007) 71 NSWLR 417.
18 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; N Henry and A Powell, *Submission 104*; Australian Sex Party, *Submission 92*. The Australian Sex Party preferred a model whereby civil remedies were available for breaches of the criminal law.
19 *Uren v John Fairfax & Sons* (1966) 117 CLR 118, 150 (Windeyer J).
20 News Corp Australia, *Submission 112*; Free TV, *Submission 109*; AMTACA, *Submission 101*; ASTRA, *Submission 99*.
21 AMTACA, *Submission 101*.
22 Guardian News and Media Limited and Guardian Australia, *Submission 80*.

this, they consider that there is '[s]ignificant potential for an harassment style of action or crime to significantly impact on bona fide journalistic activities'.[23]

15.23 Suitable defences would be needed for a harassment tort. The ALRC considers that in designing such defences, consideration should be given to ensuring the tort does not unreasonably affect responsible journalism on matters of public importance.

15.24 Describing the statutory harassment action as a tort action will provide certainty on a number of ancillary issues that will inevitably arise. However, further work would need to be done on the detailed design of a cause of action for harassment. The design of the statutory cause of action for serious invasion of privacy in this Report may provide some guidance on the design of a new harassment tort, as will harassment actions in other countries, discussed below.

Uniform state and territory legislation

15.25 The ALRC recommends that the states and territories enact uniform legislation providing for a tort of harassment.

15.26 It is unclear whether the Commonwealth has the power to enact a general tort of harassment. The Commonwealth has the power to legislate with respect to communications made over the internet or other electronic communications—under the communications power in section 51(v) of the *Australian Constitution*. However, the Constitutional basis of a more general harassment Act—covering harassment which occurs 'offline'—is less certain.

15.27 Although it is not clear, the Commonwealth's external affairs power might also support a new Commonwealth harassment Act.[24] It may be argued that harassment constitutes 'an arbitrary or unlawful interference with … privacy, family, home or correspondence',[25] under art 17 of the International Covenant on Civil and Political Rights (ICCPR) to which Australia is a party. At its broadest, a person's privacy could be considered to be interfered with by some forms of harassment. However, unlike surveillance (for example), harassment in general does not appear to be clearly recognised as involving interference with 'privacy' within the meaning of art 17 of the ICCPR. Article 17 has not been interpreted in General Comments of the Human Rights Committee, nor in case law, as involving protection from harassment.

15.28 By way of comparison, the sexual harassment provisions in the *Sex Discrimination Act 1984* (Cth) seem to be supported by the external affairs power through giving effect to provisions of the *Convention on the Elimination of all Forms of Violence against Women*.[26]

---

23 Ibid.

24 *Australian Constitution* s 51(xxix).

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

26 *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).

15.29 The states may also refer matters to the Commonwealth under s 51(xxxvii) of the *Australian Constitution*.

15.30 If the Commonwealth were to enact a cause of action for harassment, the relevant statute might include a 'reading down' provision, to attempt to ensure the validity of the law to the extent it would operate in cases that are clearly within power. Another option might be for the Commonwealth to enact more limited causes of action for harassment. For example, a tort of harassment using internet or telecommunications technology would seem to be more clearly within the Commonwealth's legislative powers.

Criminal offences for harassment

15.31 This section outlines a range of Commonwealth, state and territory criminal offences for conduct that amounts to harassment. There appear to be some gaps in state laws, and it seems Commonwealth cyber-harassment laws could be clearer and more actively enforced.

State stalking and harassment laws

15.32 State and territory laws criminalise stalking. These offences often target behaviour amounting to harassment.[27] For example, under the *Crimes Act 1958* (Vic) s 21A, a person (the offender) stalks another person (the victim)

> if the offender engages in a course of conduct [which includes any of a wide range of types of conduct] with the intention of causing physical or mental harm to the victim, including self-harm, or of arousing apprehension or fear in the victim for his or her own safety or that of any other person.

15.33 There are also state and territory offences that capture harassment at work, in family or domestic contexts, and in schools and other educational institutions. For example, the *Crimes Act 1900* (NSW) s 60E provides that it is an offence to 'assault, stalk, harass or intimidate any school student or member of staff of a school, while the student or member of staff is attending a school'.

15.34 Section 8(1) of the *Crime (Domestic and Personal Violence) Act 2007* (NSW) defines stalking as 'the following of a person about or the watching or frequenting of the vicinity of, or an approach to a person's place of residence, business or work or any place that a person frequents for the purposes of any activity'. This Act is confined to persons experiencing domestic or family violence.

15.35 Some types of serious harassment may not be caught by existing criminal offences. State and territory stalking offences, for example, are limited in their ability to protect individuals from harassment which does not involve the apprehension of actual violence. Stalking offences usually capture threatening conduct and require the

---

27 *Criminal Code* (Cth) s 189; Crimes (Domestic and Personal Violence) Act 2007 (NSW) s 13; *Criminal Code Act 1899* (Qld) s 395B; *Criminal Law Consolidation Act 1935* (SA) s 19AA; *Criminal Code Act 1924* (Tas) s 192; *Crimes Act 1958* (Vic) s 21A; *Criminal Code Act Compilation Act 1913* (WA) s 338D; *Crimes Act 1900* (ACT) s 35.

victim to apprehend actual violence or to fear harm.[28] However, persistent unwanted attention, communication or contact which does not meet this threshold could undoubtedly still cause significant harm and distress, and disrupt a person's life.

15.36 Differences between state and territory stalking offences may also undermine their effectiveness. For example, in many states, stalking requires a course of conduct covering at least two incidents,[29] but in Tasmania, stalking may be based upon one incident.[30]

15.37 Several stakeholders supported the consolidation and clarification of existing state and territory stalking criminal offences.[31] The National Children's and Youth Law Centre highlighted the need to 'address the gaps' in the current legal frameworks for cyber-bullying and harassment.[32] The Public Interest Advocacy Centre and Women's Legal Services NSW both supported a uniform approach to the criminalisation of harassment while cautioning against any consolidation process which may adopt a 'lowest common denominator' approach.[33] Uniformity in state and territory stalking provisions may deserve further consideration.

Commonwealth cyber-harassment laws

15.38 Commonwealth law criminalises cyber-harassment, but does not provide for a general offence of harassment. The Commonwealth *Criminal Code*, set out in the schedule to the *Criminal Code Act 1995* (Cth), provides for an offence of 'using a carriage service to menace, harass or cause offence'[34] and 'using a carriage service to make a threat'.[35] These would capture conduct amounting to harassment, for example, via the internet, including social media, and telephone.[36] Examples of prosecutions under this offence include posting offensive pictures and comments on Facebook tribute pages;[37] posting menacing messages on Facebook;[38] and sending repeated menacing emails.[39] The maximum penalty under s 474.17 is currently three years imprisonment. The maximum fine is $19,800 for a natural person and $99,000 for a body corporate.

---

28 See for example, *Criminal Code Act* (NT) s 189(1A).
29 *Criminal Code Act 1899* (Qld) s 359A; *Crimes Act 1900* (ACT) s 35.
30 *Criminal Code Act 1924* (Tas) s 192.
31 Women's Legal Services NSW, *Submission 115*; Free TV, *Submission 109*; Public Interest Advocacy Centre, *Submission 105*; ASTRA, *Submission 99*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; National Children and Youth Law Centre, *Submission 61*.
32 National Children and Youth Law Centre, *Submission 61*.
33 Public Interest Advocacy Centre, *Submission 105*.
34 *Criminal Code Act 1995* (Cth) sch, s 474.17.
35 Ibid sch, s 474.15.
36 At the Bullying, Young People and the Law Symposium hosted by the Alannah and Madeline Foundation in Sydney in July 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.
37 *R v Hampson* [2011] QCA 132.
38 *Agostino v Cleaves* [2010] ATSC 19.
39 *R v Ogawa* [2009] QCA 307.

15.39 There are also Commonwealth 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]

15.40 Some have suggested that the Commonwealth criminal offences for cyber-harassment might be more actively enforced, and perhaps made clearer. At the time of writing this Report, the federal Department of Communications was conducting a review into online safety for children.[41] Among other issues, the Department has been asked to consider simplifying the meaning and application of s 474.17 of the *Criminal Code*, although some stakeholders have suggested the law is appropriate. For example, the Australian Federal Police said the section was 'more than adequate to facilitate prosecution of cyber-bullying cases where appropriate', and argued that 'the breadth of section 474.17 is its strength, capturing a wide range of behaviours in a rapidly evolving online environment'.[42]

15.41 Some suggested that the law only needs to be more widely known or actively enforced, and that an education campaign might be necessary. Some commentators claim that, despite a high rate of parental reporting of cyber-bullying, there appears to be a lack of adequate knowledge or training about the applicability of the provision.[43] Facebook also supported education and awareness-raising measures to explain the application of the offence.[44] Google submitted that the problem 'is not that the laws don't exist, but rather that there is a general lack of awareness of the existing criminal and civil laws that are available'.[45]

15.42 Since the commencement of the relevant provision in 2005, and January 2014, there were 308 successful prosecutions under s 474.17 of the Commonwealth *Criminal Code* including eight prosecutions involving defendants under the age of 18.[46] The ALRC was advised by the Commonwealth Director of Public Prosecution that 74% of convictions were the result of referrals from state and territory police.[47] Only 22.6% of successful convictions were made by the Australian Federal Police. In consultations the ALRC heard concerns raised that state and territory police may be unwilling or unable to enforce criminal offences due to a lack of training and expertise in Commonwealth procedure which often differs significantly from state and territory police procedures.

---

40 *Family Law Act 1975* (Cth) s 4AB(2)(c).

41 Australian Government, 'Enhancing Online Safety for Children: Public Consultation on Key Election Commitments' (Department of Communications, January 2014). The Government has founded an Online Safety Consultative Working Group to provide advice to government on online safety issues.

42 Australian Federal Police, *Submission 67*.

43 Aashish Srivastava, Roger Gamble and Janice Boey, 'Cyberbullying in Australia: Clarifying the Problem, Considering the Solutions' (2013) 21 *International Journal of Children's Rights* 25.

44 Facebook, *Submission to Department of Communication's Enhancing Online Safety for Children Report 2014*.

45 Google, *Submission to Department of Communication's Enhancing Online Safety for Children Report 2014*.

46 Australian Government, above n 41, 21.

47 Advice correspondence, CDPP, 2 May 2014.

15.43 The Department of Communications outlined three options for reform to s 474.17. First, to retain the existing provision and implement education programs to raise awareness of its potential application. Second, to create a cyber-bullying offence with a civil penalty regime for minors. Third, to create a take-down system and accompanying infringement notice scheme to regulate complaints about online content.

Harassment laws in other countries

15.44 The *Protection from Harassment Act 1997* (UK) creates criminal offences when a person engages in a 'course of conduct' that amounts to harassment.[48] 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.[49] Harassment is defined as having occurred if 'a reasonable person in possession of the same information would think the course of conduct amounted to harassment'.[50]

15.45 Importantly, the UK Act also provides for the award of civil remedies, including injunctions and damages to victims of harassment. Courts are empowered to issue a civil non-harassment order. 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 specified'.[51]

15.46 New Zealand's *Harassment Act 1997* empowers a court to issue civil harassment restraining orders and provides for a criminal offence of harassment where a person intends to cause fear to another person.[52] A person who is prosecuted for harassment can face up to two years imprisonment.[53] 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.[54] Where the Act does not provide for compensation for victims, the common law in New Zealand has developed a tort of intrusion upon seclusion, which has been used to provide compensation for victims of harassment.[55]

15.47 A range of behaviours amounting to harassment have been successfully targeted through the UK and NZ harassment acts.[56] These include conduct by individuals such as 'trolling' on social media, posting of private photographs and the use of fake online profiles to harass individuals.

---

48 *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.

49 *Protection from Harassment Act 1997* (UK) s 1.

50 Ibid s 1(2).

51 Ibid s 11.

52 *Harassment Act 1997* (NZ) s 8.

53 Ibid.

54 Ibid s 9.

55 *C v Holland* [2012] 3 NZLR 672.

56 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.

15.48 At the time of writing this Report, New Zealand's government was also considering legislation to tackle 'harmful digital communications' by way of 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.[57] This offence would be punishable by up to three months imprisonment or a NZ$2,000 fine.

15.49 Singapore's *Protection from Harassment Act 2014* criminalises stalking and other forms of anti-social behaviour. The Act provides for a civil action of harassment whereby plaintiffs can receive an award of damages. Courts are also empowered under the Act to issue civil protection orders against offenders and have the power to remove offending material from a platform such as the internet.[58]

15.50 Other jurisdictions have enacted legislation to specifically target cyber-harms and so-called 'revenge pornography'.[59] Revenge pornography is understood as the collection and distribution of sexually graphic images of an individual without their consent, with the deliberate intention of embarrassing, demeaning and distressing that individual. These images are often taken consensually during an intimate relationship.

15.51 For example, 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'.[60] Cyber-bullying is defined 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.[61]

15.52 In an action for cyber-bullying under this Act, a court may award damages including general, special, aggravated and punitive damages.[62] A court may also issue an injunction,[63] or make an order that the court considers 'just and reasonable in the circumstances'.[64]

15.53 These laws provide a useful model for Australian legislatures when enacting a statutory tort of harassment, or other harassment legislation.

---

57 Harmful Digital Communications Bill 2013 (NZ) cl 19.

58 Prior to the enactment of the *Protection from Harassment Act 2014,* the *Miscellaneous Offences (Public Order and Nuisance) Act* ch 184, ss13A–D criminalised offline harassment.

59 Eg, New Jersey legislation criminalises the reproduction or disclosure of images of sexual contact without consent: *NJ Rev Stat § 2C:14-9 (2013)*.

60 *Cyber-Safety Act*, SNS 2013, c 2 2013 s 3(b).

61 Ibid.

62 *Cyber-Safety Act 2013* (SNS) s 22(1)(a).

63 Ibid s 22(1)(b).

64 Ibid s 22(1)(c).

16. New Regulatory Mechanisms

Contents

Summary 309
Privacy Commissioner investigations for serious invasions of privacy 310
Deletion, removal and de-identification 312
Complaints about media invasions of privacy 314
Conciliation process 316
Amicus curiae and intervener functions 317
An amicus curiae function for the Commissioner 318
An intervener function for the Commissioner 318
Deletion of personal information 319
Review of the small business exemption 321

Summary

16.1 This chapter sets out recommendations about new regulatory mechanisms to reduce and redress serious invasions of privacy. The new regulatory powers the ALRC recommends in this chapter are not intended to be an alternative to a statutory tort for serious invasions of privacy—although, in the absence of a statutory tort, the new regulatory powers would increase the legal protection of privacy. Rather, the new regulatory powers would complement a statutory tort, providing a low cost alternative to litigation, which may, in some cases, lead to a satisfactory outcome for parties.

16.2 The ALRC recommends that consideration be given to conferring extended powers on the Privacy Commissioner to investigate complaints about serious invasions of privacy. This would provide a forum for consideration of complaints about serious invasions of privacy without requiring parties to commit the time and resources that might be needed for court proceedings. Under these extended powers, the Commissioner could be given the power to recommend the non-publication or removal of private information from publication. However, court action would be required to enforce such a recommendation.

16.3 The ALRC also recommends conferring additional functions on the Privacy Commissioner to act as amicus curiae or intervener in court proceedings, with the leave of the court, where the Commissioner considers it appropriate.

Privacy Commissioner investigations for serious invasions of privacy

Recommendation 16–1 The Commonwealth Government should consider extending the Privacy Commissioner's powers so that the Commissioner may investigate complaints about serious invasions of privacy and make appropriate declarations. Such declarations would require referral to a court for enforcement.

16.4 There may be a number of benefits to empowering the Privacy Commissioner to investigate complaints about serious invasions of privacy, in addition to providing a cause of action allowing individuals to undertake court proceedings for serious invasion of privacy.[1] These benefits may include:

- greater accessibility and lower cost of a complaints mechanism as compared to court proceedings;[2]
- use of the Commissioner's experience and expertise in handling privacy complaints;[3]
- benefits of providing the Commissioner with a formal role in addressing serious invasions of privacy, including the benefits of avoiding the fragmentation that might occur if the Commissioner had no such role;[4] and
- significant public awareness of the Commissioner in relation to privacy concerns.[5]

16.5 The mechanism might face challenges, including:

- the need for additional resources to be provided to the Commissioner; and
- the limitations of exemptions in the *Privacy Act 1988* (Cth), which generally does not apply to individuals, small businesses or media organisations.

16.6 A power for the Commissioner to investigate complaints about serious invasions of privacy could be integrated with the Commissioner's existing powers to investigate

---

1 Under the *Privacy Act 1988* (Cth), privacy functions are conferred on the Australian Information Commissioner. However, in the 2014 Budget, the Australian Government announced an intention to disband the Office of the Australian Information Commissioner. The Privacy Commissioner would hold an independent statutory position within the Australian Human Rights Commission. At the time of writing, these changes have not taken place. In this Report, the ALRC uses the terms 'Privacy Commissioner' and 'Commissioner' to refer to the person exercising the privacy functions under the *Privacy Act*.

2 ACCAN, *Submission 106*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

3 Australian Privacy Foundation, *Submission 110*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

4 Australian Privacy Foundation, *Submission 110*; Office of the Australian Information Commissioner, *Submission 90*; G Greenleaf, *Submission 76*.

5 Office of the Australian Information Commissioner, *Submission 90*.

complaints about breaches of information privacy. The *Privacy Act* currently provides for complaints to be made to the Commissioner where there may have been an 'interference with the privacy of an individual'.[6] Under the Act, an interference with the privacy of an individual will have occurred where there has been a breach of:

- any of the Australian Privacy Principles (APPs);[7]
- a registered APP code;[8]
- the credit reporting provisions or the registered CR code;[9]
- certain rules relating to tax file numbers;[10] or
- certain provisions of other legislation, where that legislation provides that a particular act or conduct is an interference with the privacy of an individual for the purposes of the *Privacy Act*.[11]

16.7 The *Privacy Act* could be amended to provide that a serious invasion of privacy would also be an interference with the privacy of an individual. This approach was suggested by Professor Graham Greenleaf, who submitted that, if an Act providing for the tort for serious invasions of privacy were enacted:

> a new sub-section 13(6) should be added to the *Privacy Act 1988*: '(6) A serious invasion of privacy under the [Act providing the statutory tort] is an interference with the privacy of an individual …'[12]

16.8 In the event that an interference with the privacy of an individual occurs, the Commissioner has the power to receive and investigate a complaint from the individual whose privacy has been interfered with, or to begin an 'own motion investigation' of the interference.[13] Following an investigation, the Commissioner may make a determination including various declarations, such as a declaration that the respondent to the complaint must take specified actions, a declaration that the respondent must take steps to redress any loss or damage suffered by the complainant, or a declaration that the complainant is entitled to a specified amount of compensation.[14] A determination following an investigation is enforceable through the Federal Court and Federal Circuit Court, on application of either the complainant or the Commissioner.[15] If a serious invasion of privacy was also an interference with the privacy of an

---

6 *Privacy Act 1988* (Cth) s 36.
7 Ibid s 13(1).
8 Ibid.
9 Ibid s 13(2).
10 Ibid s 13(4).
11 An interference with the privacy of an individual can arise, for example, under *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 35L.
12 G Greenleaf, *Submission 76*. As noted in Professor Greenleaf's submission, if a new section in the *Privacy Act* referred to 'an act', a range of exemptions, such as the media exemption under s 7B(4), would take effect, limiting the effect of the new provisions.
13 *Privacy Act 1988* (Cth) ss 36, 40.
14 Ibid s 52(1). Similar declarations may be made in the case of an own motion investigation: ibid s 52(1A).
15 *Privacy Act 1988* (Cth) s 55A.

individual under the *Privacy Act*, these same determinations could be made following a complaint to the Commissioner about a serious invasion of privacy.

16.9 Further consequences of an interference with the privacy of an individual under the *Privacy Act* include:

- where an interference with the privacy of an individual is 'serious' or 'repeated', the Commissioner is empowered to seek civil pecuniary penalties from the Federal Court or Federal Circuit Court;[16] and
- where a person has engaged in, or is engaging in, conduct that contravenes the Act, an individual or the Commissioner may apply to the Federal Court or the Federal Circuit Court for an injunction.[17]

16.10 The media, small businesses and individuals are not exempt from liability under the tort for serious invasions of privacy discussed in Part 2 of this Report. However, they are generally exempt from regulation under the *Privacy Act*.[18] If the Commissioner's functions were extended to hear complaints about serious invasions of privacy, this should include complaints about invasions of privacy by the media, small business and individuals. There would be little value in extending the Commissioner's powers if the existing exemptions also applied to complaints made under the extended powers. The amendments to the *Privacy Act* would need to make this clear.

16.11 Before any extended powers were conferred on the Commissioner, consideration would need to be given to whether or not the extended powers would require the Commissioner to exercise a judicial power. The *Australian Constitution* restricts the conferral of judicial powers on non-judicial bodies.[19] Although 'judicial power' has not been exhaustively defined, one characteristic of a judicial power is its binding nature.[20] A determination under the *Privacy Act* complaints process is not binding, since it must be enforced through action in the Federal Court or Federal Magistrates Court. This suggests that the *Privacy Act* does not confer judicial powers on the Commissioner.[21]

Deletion, removal and de-identification

16.12 The Commissioner's existing powers in relation to an interference with the privacy of an individual include a power to make a declaration that the respondent

16 Ibid ss 13G, 80W.

17 Ibid s 98. This provision appears to be rarely used. However, it provides a useful means for an individual to seek relief for a breach of the *Privacy Act*.

18 For the media exemption, see *Privacy Act* s 7B(4). For the small business exemption, see *Privacy Act* ss 6C(1), 6D. For the exemption for individuals, see *Privacy Act* s 16. Individuals will also generally fall outside the definition of relevant types of entities; see, for example, *Privacy Act* s 6(1) (definition of 'APP entity').

19 *R v Kirby; ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254.

20 *Brandy v Human Rights & Equal Opportunity Commission* (1995) 183 CLR 245, 268 (Deane, Dawson, Gummow, McHugh JJ).

21 An example of a regulator being found to have exercised a judicial function can be found in *Today FM (Sydney) v Australian Communications and Media Authority* (2014) 307 ALR 1. There, the Full Federal Court found that the Australian Communications and Media Authority had exercised a judicial power in finding that a broadcaster had breached a licence condition by committing a criminal offence.

'must not repeat or continue such conduct'[22] or a declaration that the respondent 'must take specified steps within a specified period to ensure that such conduct is not repeated or continued'.[23] It appears that such declarations may require the respondent to delete, remove or de-identify personal information.

16.13 A number of stakeholders supported the introduction of a regulator take-down mechanism.[24] However, there is a risk that such a system may have an undesirably chilling effect on online freedom of expression, and any such power would need to balance the interests of the complainant against the interests of the party in publishing the material and broader public interests. The power would need to be exercised with caution.

16.14 The existing availability of declarations that a respondent to a complaint not repeat or continue the conduct complained about may provide a suitable mechanism for individuals to seek to have information removed, while avoiding the chilling effect that may come from other take-down mechanisms. There may be no need to confer substantial new powers on the Commissioner, beyond the power to investigate complaints about serious invasions of privacy. Furthermore, a declaration that a respondent must not repeat or continue the conduct complained about would not, by itself, be enforceable; the complainant would need to apply to the Federal Court or Federal Circuit Court for enforcement if the respondent refused to comply with the Commissioner's declaration.

16.15 Several stakeholders were opposed to any take-down mechanism on the grounds that such a mechanism may, in some cases, be ineffective.[25] The Australian Mobile Telecommunications Association and Communications Alliance submitted that, given the speed and volume at which content is created and published online,

> the implementation of such a system is likely to be impossible to comply with and costly and time-consuming for government and business, as well as being ineffective in relation to user-generated content.[26]

16.16 Several other organisations noted the difficulty of effectively removing information that has become more widely available,[27] or where the respondent is located overseas.[28]

---

22 *Privacy Act 1988* (Cth) s 52(1)(b)(i).

23 Ibid s 52(1)(b)(ia).

24 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; Pirate Party of Australia, *Submission 119*; Women's Legal Services NSW, *Submission 115*; T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Redfern Legal Centre, *Submission 94*; Australian Sex Party, *Submission 92*; J Chard, *Submission 88*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*.

25 Telstra, *Submission 107*; AMTACA, *Submission 101*; Australian Bankers' Association, *Submission 84*.

26 AMTACA, *Submission 101*.

27 Australian Communications and Media Authority, *Submission 121*; Pirate Party of Australia, *Submission 119*.

28 Australian Communications and Media Authority, *Submission 121*; Pirate Party of Australia, *Submission 119*; UNSW Cyberspace Law and Policy Community, *Submission 98*; Office of the Australian Information Commissioner, *Submission 90*.

16.17 The ALRC acknowledges that a take-down mechanism may have limited effect in cases where material has been widely disseminated or where material is hosted overseas. However, the ALRC considers that the possibility of the mechanism having limited effect in some cases is not, in itself, a reason not to make the mechanism available in those cases where it may be effective. This is particularly the case given that the Commissioner is already empowered to make the relevant declarations under the existing provisions of the *Privacy Act*.

Complaints about media invasions of privacy

16.18 In the Discussion Paper, the ALRC proposed an extension of the powers of the Australian Communications and Media Authority (ACMA). However, the ALRC has concluded that such declarations would be more appropriately made by the Privacy Commissioner.

16.19 The proposed extension would have allowed the ACMA to make a declaration that the complainant was entitled to a specified amount of compensation, in response to a complaint about a serious invasion of privacy in breach of a broadcasting code of conduct. This would have been equivalent to the powers of the Privacy Commissioner.

16.20 Although the Commissioner already has such powers under the *Privacy Act*,[29] 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.[30] The result is that an individual whose privacy is invaded by a broadcaster has little access, if any, to regulatory mechanisms providing for compensatory redress.

16.21 The ACMA's powers with respect to broadcasting codes of conduct are provided under the *Broadcasting Services Act 1992* (Cth). These 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.

16.22 If a code is breached, the ACMA may: determine an industry standard;[31] make compliance with the code a condition of the broadcaster's licence;[32] or accept an enforceable undertaking from the broadcaster that the broadcaster will comply with the code.[33] Further consequences exist, including civil penalties, criminal penalties and suspension or cancellation of a broadcaster's licence, for a breach of a standard,[34] a licence condition[35] or an enforceable undertaking.[36] If a complaint is made against the

---

29 Under *Privacy Act* s 52(1A)(d), 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.

30 *Privacy Act 1988* (Cth) s 7B(4).

31 *Broadcasting Services Act 1992* (Cth) s 125.

32 Ibid s 44.

33 Ibid s 205W.

34 Ibid pt 9B div 5.

35 Ibid pt 10 div 3.

36 Ibid pt 14D.

ABC or SBS, 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.[37]

16.23 There was significant opposition from broadcasters and media organisations to the proposal to extend the ACMA's powers. A key argument among broadcasters was that the proposal was inconsistent with the ACMA's existing role as the manager of a co-regulatory scheme which has the goal of 'encouraging broadcasters to reflect community standards'.[38] The Australian Subscription Television and Radio Association (ASTRA) submitted, for example, that

> Such a proposal would represent a significant shift in the functions and powers of the ACMA. The ACMA does not currently have the power to order compensation be paid to an individual in relation to a breach of any broadcasting code of practice, broadcasting licence condition or any other obligation on broadcasters established under the *Broadcasting Services Act 1992* (BSA). This does not represent a 'limitation' of the ACMA's powers under the BSA—rather, it reflects … the intention of the regulatory framework for broadcasting established by Parliament.[39]

16.24 Stakeholders—including the ACMA itself—were also concerned that, if the ACMA were empowered to suggest compensation for invasions of privacy, there would be increased fragmentation of privacy protections. This fragmentation would result in confusion and complexity for individuals and organisations:

- different regulators would regulate privacy in different sectors;[40]
- the new power would apply only to breaches of broadcasting codes involving serious invasions of privacy, and not to other breaches of the codes;[41]
- within the media sector, different regulatory schemes would apply to different forms of media.[42]

16.25 The risks of fragmentation under the proposed ACMA power are, to a large extent, an unavoidable consequence of the fragmented nature of media regulation in Australia. While the ACMA has powers relating to broadcast media under the *Broadcasting Services Act*, regulation of non-broadcast media is a matter of self-regulation by the Australian Press Council.

16.26 Although a number of stakeholders were supportive of the proposed ACMA power,[43] the ALRC has determined, in view of the changes to the existing regulatory landscape that would be involved, not to proceed with the proposal.

---

37 Ibid ss 150–152.
38 Australian Communications and Media Authority, *Submission 121*.
39 ASTRA, *Submission 99*. See also SBS, *Submission 123*; Free TV, *Submission 109*.
40 Office of the Australian Information Commissioner, *Submission 90*.
41 Australian Communications and Media Authority, *Submission 121*.
42 SBS, *Submission 123*.
43 Domestic Violence Legal Service and North Australian Aboriginal Justice Agency, *Submission 120*; T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; G Greenleaf, *Submission 76*; D Butler, *Submission 74*.

16.27 The ACMA suggested, as an alternative to the proposed new power, that the ACMA should be empowered:

> [to] refer found privacy breaches to the [Office of the Australian Information Commissioner] to make a determination as to the seriousness of the breach, to provide for conciliation and to make [a] declaration as to the amount of any compensation payable.[44]

16.28 Noting that the ACMA's role, as discussed above, is not to provide individual redress, the ALRC agrees that the Privacy Commissioner is an appropriate body to make declarations relating to compensation for serious invasions of privacy. However, if the Commissioner's powers are extended to include investigating complaints about serious invasions of privacy by broadcasters or other media, the media exemption of the *Privacy Act* should not apply in respect of complaints about serious invasions of privacy. The media exemption could, however, continue to apply in respect of information privacy under others parts of the *Privacy Act*.

Conciliation process

16.29 An alternative to extending the Commissioner's existing investigation powers is a conciliation process operated by the Commissioner. Such a conciliation process could be similar to that used by the Australian Human Rights Commission (AHRC). Under pt IIB of the *Australian Human Rights Commission Act 1986* (Cth), the President of the AHRC may attempt to conciliate a complaint alleging unlawful discrimination. In certain circumstances—for example, where the President of the AHRC is satisfied that there is no reasonable prospect of the matter being settled by conciliation—a complaint may be taken to the Federal Court or the Federal Circuit Court.[45]

16.30 The Law Institute of Victoria expressed a preference for this type of model, whereby

> the Privacy Commissioner would be providing alternative dispute resolution services, rather than making a finding about the claim. If the dispute is not resolved, the plaintiff would be required to pursue the claim through the courts.[46]

16.31 A conciliation process would not be binding on parties. However, conciliation may lead to satisfactory outcomes for both parties, without the need to resort to court proceedings. In the event that conciliation was unsuccessful, the complaint could be taken to a court under the tort for serious invasions of privacy, if that statutory tort were enacted.

16.32 The conciliation process would thus provide an initial low cost mechanism for resolving disputes. Such a process need not be mandatory. However, the ALRC recommends that a failure to make a reasonable attempt at conciliation should be a factor considered by a court in the event that damages were to be awarded.[47]

---

44 Australian Communications and Media Authority, *Submission 121*.

45 The usefulness of the AHRC's conciliation function as a model was noted by the Media and Communications Committee of the Law Council of Australia, *Submission 124*.

46 Law Institute of Victoria, *Submission 96*.

47 See Ch 12 and in particular Rec 12–2.

Amicus curiae and intervener functions

Recommendation 16–2 The following functions should be conferred on the Privacy Commissioner:

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

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

16.33 The ALRC recommends that the Privacy Commissioner be given new functions to act as amicus curiae ('friend of the court') or to intervene in legal proceedings relating to serious invasions of privacy. These functions would be additional to a range of existing functions conferred on the Commissioner under *Privacy Act 1988* (Cth) ss 27–29, including: preparing guidance about the Act; monitoring the privacy impacts of new laws; and providing advice about the operation of the Act.

16.34 These amicus curiae and intervener functions would be similar to functions conferred on other administrative bodies—such as the Australian Competition and Consumer Commission (ACCC), the Australian Securities and Investments Commission (ASIC) and the AHRC.

16.35 Stakeholders who commented on the ALRC's proposal were generally supportive of the Commissioner being given amicus curiae and intervener functions.[48] The Office of the Australian Information Commissioner (OAIC) suggested that it should be given amicus curiae and intervener roles in its submission to the Issues Paper.[49] In its submission to the Discussion Paper, the OAIC noted that amicus curiae and intervener roles would be particularly appropriate if the OAIC had a greater role in hearing complaints about serious invasions of privacy.[50]

16.36 It is likely that, if a statutory cause of action for serious invasions of privacy were enacted, there would be an increase in the number of claims relating to the intentional disclosure of personal information. In such cases, the Commissioner may be in a position to assist the court as amicus curiae, or to represent the Commissioner's interests as an intervener.

---

48 T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Public Interest Advocacy Centre, *Submission 105*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; Guardian News and Media Limited and Guardian Australia, *Submission 80*; G Greenleaf, *Submission 76*.

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

50 Office of the Australian Information Commissioner, *Submission 90*.

An amicus curiae function for the Commissioner

16.37 The role of an amicus curiae is to assist the court 'by drawing attention to some aspect of the case which might otherwise be overlooked.'[51] 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'.[52] The amicus is not a party to the proceedings and is not bound by the outcome of the proceedings. This role does not extend to introducing evidence to the court, although an amicus may be permitted to lead non-controversial evidence in order to 'complete the evidentiary mosaic'.[53]

16.38 An example of legislation conferring an amicus curiae function on an administrative body is s 46PV of the *Australian Human Rights Commission Act 1986* (Cth). This section allows an individual ('special-purpose') Commissioner within the AHRC to act as amicus 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.

16.39 Importantly, an amicus curiae does not have a legal interest in the outcome of the proceedings. Any person with a legal interest in proceedings may, with the leave of the court, intervene in the proceedings.

An intervener function for the Commissioner

16.40 The role of amicus curiae can be distinguished from the role of an intervener. While the role of amicus is to assist the court, the role of an intervener is to represent the intervener's own legal interests in proceedings.

16.41 An intervener's legal interests may be affected in a number of ways. 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 property interests of the intervener. The intervener's interests may also be indirectly affected: for example, the court's decision might have an effect on the future

---

51 *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.

52 *Levy v Victoria* (1997) 189 CLR 579, 604 (Brennan CJ).

53 *Bropho v Tickner* (1993) 40 FCR 165, 172 (Wilcox J).

interpretation of laws affecting the intervener.[54] Under the ALRC's recommendation, a court might, for example, give leave to the Commissioner to intervene in a case that would have future repercussions for the work of the Commissioner.

16.42 Functions to intervene are conferred upon a number of administrative bodies. For example, s 11(1)(o) of the *Australian Human Rights Commission Act* confers an intervention function on the AHRC:

> where the 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.[55]

16.43 The ACCC has an intervention function in relation to proceedings under the *Competition and Consumer Act 2010* (Cth).[56] ASIC has an intervention function in relation to proceedings about consumer protection in financial services.[57]

Deletion of personal information

16.44 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.[58] It is therefore important that individuals be able to exercise a degree of control over their personal information, especially information that they may themselves have provided previously. In particular, individuals should be empowered to have their personal information destroyed—or, at a minimum, de-identified—when appropriate.

16.45 In the Discussion Paper, the ALRC proposed that a new APP be inserted into the *Privacy Act*, that would:

- require APP entities to provide a simple mechanism for an individual to request destruction or de-identification of personal information that the individual had provided to the entity; and
- require APP entities to take reasonable steps in a reasonable time to comply with such a request, subject to suitable exceptions, or to provide the individual with reasons for non-compliance.

16.46 The ALRC argued that the proposed APP would complement existing APPs that require APP entities to correct personal information (the correction principle)[59] and to destroy or de-identify personal information when it is no longer required for a relevant

---

54 *Levy v Victoria* (1997) 189 CLR 579, 601–602 (Brennan CJ).

55 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 Act 2004* (Cth) s 53(1)(g).

56 *Competition and Consumer Act 2010* (Cth) s 87CA.

57 *Australian Securities and Investments Commission Act 2001* (Cth) s 12GO.

58 National Children and Youth Law Centre, *Submission 61*; Google, *Submission 54*; Australian Privacy Foundation, *Submission 39*; B Arnold, *Submission 28*.

59 *Privacy Act 1988* (Cth) APP 13.

purpose (the security principle).[60] Although the existing APPs provide some protection, they do not incorporate a mechanism allowing individuals to request destruction or de-identification.

16.47 The proposal was supported by a number of stakeholders.[61] Others were opposed to it,[62] noting the existing correction and security principles[63] and the need to retain personal information for business purposes, such as billing.[64] Some stakeholders were not opposed to the proposal, subject to particular concerns being met.[65]

16.48 The OAIC opposed the proposal. The OAIC noted that it would not be relevant to most information held by Australian Government agencies due to the retention requirements of the *Archives Act 1983* (Cth). The OAIC also noted that, in addition to the existing correction and security principles, other principles restrict the circumstances in which an APP entity may collect or disclose information:[66]

> The requirement in the proposed APP for an organisation to destroy or de-identify the personal information, in circumstances where the organisation is still authorised to use or disclose it under the Privacy Act … has the potential to impose a significant burden on the organisation and disrupt its business practices. The OAIC considers that the existing measures in the APPs balance the need to give an individual control over the handling of their personal information with the regulatory burden on entities when carrying out their functions and activities, and that the additional burden in the proposed new APP is unjustified and unnecessary.[67]

16.49 The OAIC also submitted that, rather than introducing a new APP into the *Privacy Act*, the OAIC could

> issue additional guidance on an entity's obligations under the existing APPs to destroy or de-identify personal information and good privacy practice when an individual requests the entity to destroy or de-identify their personal information.

16.50 The ALRC accepts that the existing APPs require the destruction or de-identification of personal information in many circumstances. However, there are scenarios in which an APP entity may be able to retain personal information even after the individual has ceased their business relationship with the APP entity. For example, if the purpose of the collection includes the APP entity's own statistical research, it is not clear that the entity would be required to destroy or de-identify the information

---

60 Ibid APP 11.2.

61 T Butler, *Submission 114*; Australian Privacy Foundation, *Submission 110*; Office of the Victorian Privacy Commissioner, *Submission 108*; Australian Communications Consumer Action Network, *Submission 106*; Australian Sex Party, *Submission 92*; S Higgins, *Submission 82*; I Turnbull, *Submission 81*; G Greenleaf, *Submission 76*.

62 Telstra, *Submission 107*; AMTACA, *Submission 101*; ASTRA, *Submission 99*; Office of the Australian Information Commissioner, *Submission 90*; Interactive Games and Entertainment Association, *Submission 86*; Australian Bankers' Association, *Submission 84*.

63 AMTACA, *Submission 101*; Interactive Games and Entertainment Association, *Submission 86*.

64 ASTRA, *Submission 99*.

65 Australian Interactive Media Industry Association (AIMIA), *Submission 125*; Insurance Council of Australia, *Submission 102*.

66 *Privacy Act 1988* (Cth) APPs 3, 6.

67 Office of the Australian Information Commissioner, *Submission 90*.

unless and until the research was concluded, regardless of the duration or purpose of the research.

16.51 However, the ALRC accepts that the introduction of a new APP may require further consideration of the existing APPs, and that the effect of the recent reforms of the *Privacy Act* should be determined before further reforms take place.[68] The ALRC is not, therefore, recommending the introduction of a new APP. The ALRC remains concerned, however, that the existing APPs do not require an entity to provide a simple mechanism allowing an individual to request the destruction or de-identification of personal information.

Review of the small business exemption

16.52 The APPs under the *Privacy Act* regulate the handling of personal information by APP entities: government agencies and organisations.[69] Notably, small businesses with an annual turnover of less than $3 million[70] are exempt from the definition of 'organisation' and hence 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.[71]

16.53 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 substantial benefits for the protection of privacy.[72]

16.54 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.[73]

16.55 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 2008. The ALRC acknowledges that simply removing the small

---

68 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
69 *Privacy Act 1988* (Cth) s 6(1) (definition of 'APP entity').
70 Ibid ss 6C, 6D.
71 Ibid ss 6D, 6E, 6EA.
72 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) Rec 39–1.
73 '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).

business exemption would increase compliance costs for small businesses. However, options other than simply removing the exemption are available.

16.56 The Productivity Commission may be well-placed to investigate the likely impacts on small businesses if the small business exemption were removed, or if other options for protecting personal information held by small businesses were introduced. Such an investigation could give detailed consideration to the application of data protection laws to small businesses in other jurisdictions[74] as well as other options for improving the protection of personal information held by small business. These options might include, for example, the introduction of an accreditation scheme to encourage small businesses to opt in[75] to the *Privacy Act* in order to demonstrate a commitment to good privacy practices, or a limitation of the small business exemption so that small businesses handling sensitive information[76] or financial information would not be exempt from the Act.

74 For example, small business are bound by the *Data Protection Act 1998* (UK).

75 Small businesses may elect to be treated as organisations under s 6EA of the *Privacy Act 1988* (Cth).

76 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: Ibid s 6(1) (definition of 'sensitive information').

Consultations

Name	Location
The Hon Justice Peter Applegarth, Supreme Court of Queensland	Sydney
Arts Law Centre	Sydney
Australian Bankers' Association	Sydney
Australian Broadcasting Corporation (ABC)	Sydney
Australian Communications and Media Authority (ACMA)	Sydney
Australian Chamber of Commerce and Industry	Sydney
Australian Federal Police	Canberra
Association for Data-driven Marketing & Advertising	Sydney
Australian Government, Attorney-General's Department	Canberra
Australian Government, Attorney-General's Department	Sydney
Australian Government, Department of Communications	Canberra
Australian Government Solicitor, Office of General Counsel	Canberra
Australian Institute of Professional Photographers	Sydney
Australian Privacy Foundation and NSW Council for Civil Liberties	Sydney
Paul Barry, Journalist, ABC	Sydney
Civil Aviation Safety Authority (CASA)	Canberra
Commercial Radio Australia	Sydney
Communications and Media Law Association Inc (CAMLA)	Sydney

Name	**Location**
Corrs Chambers Westgarth Lawyers	Sydney
Emeritus Professor Jim Davis, Australian National University	Canberra
Professor Julian Disney AO, Australian Press Council	Sydney
Facebook, Mia Garlick	Sydney
Facebook, Mia Garlick and Rob Sherman	Sydney
Free TV	Sydney
Patrick George, Partner, Kennedys Law	Sydney
Jed Goodfellow, PhD candidate, Macquarie University Law School	Sydney
Thomas Gregory, House of Representative Standing Committee on Social, Policy and Legal Affairs, Inquiry Secretary	Canberra
Dr Elizabeth Coombs, NSW Privacy Commissioner, Information and Privacy Commission, New South Wales	Sydney
Candice Jansz-Richardson, PhD Candidate Monash University and Office of the Victorian Privacy Commissioner, Youth Advisory Group	Melbourne
Law Council of Australia	Sydney
Law Council of Australia, Media and Communications Committee	Sydney
Law Institute of Victoria	Melbourne
Law Institute of Victoria	Sydney
Law Society of New South Wales, Young Lawyers	Sydney
The Hon Justice Mark Leeming, New South Wales Court of Appeal	Sydney
Legal Roundtable: The Hon Justice Peter Applegarth, Supreme Court of Qld (Member of Advisory Committee); Peter Bartlett, Partner, Minter Ellison; Tom Blackburn SC, Barrister; Bruce Burke, Partner, Banki Haddock Fiora; Sandy Dawson, Barrister; the Hon Justice	Sydney

Name	**Location**
John Middleton, Federal Court of Australia (Part-time Commissioner); the Hon Henric Nicholas QC, Barrister (Member of Advisory Committee); the Hon Justice Steven Rares, Federal Court of Australia; the Hon Justice Ruth McColl, NSW Court of Appeal; the Hon Justice Anthony Meagher, NSW Court of Appeal; the Hon Justice Carolyn Simpson, Supreme Court of NSW; Bruce McClintock SC, Barrister; Leanne Norman, Partner, Banki Haddock Fiora; Tim Senior, Senior Associate, Banki Haddock Fiora; Kieren Smark SC, Barrister	
London Roundtable: Professor Tanya Aplin; Emeritus Professor Eric Barendt, UCL; John Battle, General Counsel; Iain Christie, Barrister; Lee Dobbs, Solicitor; Dr David Erdos; Dr Kirsty Hughes; Perry Keller, KCL; Keith Mathieson; Gavin Millar QC; Gill Phillips; Professor Gavin Phillipson; Andrew Scott, LSE; Prof Dr Eloise Scotford KCL; Sir Stephen Sedley; Hugh Tomlinson QC; the Hon Mr Justice Michael Tugendhat; Mark Warby QC	London
Media Roundtable: ASTRA, Commercial Radio Australia, Free TV, News Corp Australia, SBS	Sydney
Megan Mitchell, National Children's Commissioner	Sydney
Bruce McClintock SC	Sydney
The Hon Justice John Eric Middleton, Federal Court of Australia, Part-time Commissioner	Sydney
Tara McNeilly, Australian Government Solicitor, ALRC Privacy Advisory Committee Member	Canberra
National Australia Bank (NAB)	Sydney
National Children's and Youth Law Centre	Sydney
National E-Health Transition Authority	Sydney
National Farmers' Federation	Canberra
New South Wales Farmers' Association	Sydney

Name	**Location**
NSW Health	Sydney
NSW Police	Sydney
Clem Newton-Brown MP, Member for Prahran, Chair of Victorian Parliament Law Reform Committee	Melbourne
Office of the Australian Information Commissioner	Sydney
Office of the Information Commissioner, Queensland	Sydney
Office of Parliamentary Counsel	Canberra
Professor David Partlett, Dean and Asa Griggs Calder Professor of Law, Emory University School of Law	Canberra
Office of the Victorian Privacy Commissioner	Melbourne
Professor Megan Richardson, Melbourne Law School	Sydney
Michael Rivette, Barrister	Sydney
Associate Professor David Rolph, Sydney Law School, University of Sydney	Sydney
South Australian Law Reform Institute	Sydney
South Australian Privacy Committee	Canberra
Special Broadcasting Service (SBS)	Sydney
Telstra	Melbourne
Richard Thomas CBE, former UK Data Protection Commissioner	Sydney
Monash University academics: Associate Prof David Lindsay, Associate Prof Moira Paterson, and Dr Normann Witzleb	Melbourne
Tim Wilson, Human Rights Commissioner, Australian Human Rights Commission	Sydney
Women's Legal Service NSW	Sydney

Abbreviations

AAT	Administrative Appeals Tribunal
ABA	Australian Bankers' Association
ABS	Australian Bureau of Statistics
ACAT	ACT Civil and Administrative Tribunal
ACCAN	Australian Communications Consumer Action Network
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ADR	Alternative dispute resolution
AFP	Australian Federal Police
AIPP	Australian Institute of Professional Photographers
AISA	Australian Information Security Association
ALRC	Australian Law Reform Commission
AMTACA	Australian Mobile Telecommunications Association and Communications Alliance Ltd
APC	Australian Press Council
APF	Australian Privacy Foundation
APP	Australian Privacy Principle
ASTRA	Australian Subscription Television and Radio Association
COAG	Council of Australian Governments
CASA	Civil Aviation and Safety Authority

CEDAW	Convention on the Elimination of all Forms of Discrimination Against Women
IGEA	Interactive Games and Entertainment Association
ICCPR	International Covenant on Civil and Political Rights
NeHTA	National E-Health Transition Authority
NFF	National Farmers' Federation
NSW	New South Wales
NSW LEC	NSW Land and Environment Court
NSWLRC	New South Wales Law Reform Commission
NSWSC	New South Wales Supreme Court
OAIC	Office of the Australian Information Commissioner
OVPC	Office of the Victorian Privacy Commissioner
PIAC	Public Interest Advocacy Centre
QCAT	Queensland Civil and Administrative Appeals Tribunal
QPEC	Queensland Planning and Environment Court
SAT	State Administrative Tribunal of Western Australia
SCLG	Standing Council on Law and Justice
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
VCAT	Victorian Civil and Administrative Appeals Tribunal
VLRC	Victorian Law Reform Commission