3. Overview of Current Law

Contents

Summary

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

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

Information privacy

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

3.4 The *Privacy Act* provides 13 'Australian Privacy Principles' (APPs) that set out the broad requirements on collection, use, disclosure and other handling of personal information.[3] The APPs bind only 'APP entities'—primarily Australian Government agencies and large private sector organisations with a turnover of more than $3 million. Certain small businesses are also bound, such as those that provide health services and those that disclose personal information to anyone else for a benefit, service or advantage.[4] Generally, individuals are not bound by the *Privacy Act*.[5]

3.5 Personal information is defined in s 6(1) of the Act as information or opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not in material form.

3.6 A breach of an APP in respect of personal information is an 'interference with the privacy of an individual'. Serious or repeated contraventions may give rise to a civil penalty order.[6]

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

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

---

1 The *Privacy Act 1988* (Cth) has been the subject of recent reforms following the ALRC's previous Privacy Inquiry. A number of recommendations made in ALRC Report 108 have been implemented by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), key provisions of which came into effect on 14 March 2014.

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

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

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

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

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

7 Ibid ss 36, 40.

8 Ibid s 40(1A).

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

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

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

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

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

3.11 State and territory legislation creates information privacy requirements similar to those under the *Privacy Act*, with application to state and territory government agencies, as well as (variously) local councils, government-owned corporations and universities.[16]

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

---

9 Ibid s 52(1).
10 Ibid s 55A.
11 Ibid s 98.
12 The ALRC is aware of only two successful applications: *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* [2004] FCA 637 (21 May 2004); *Smallbone v New South Wales Bar Association* [2011] FCA 1145 (6 October 2011).
13 *Privacy Act 1988* (Cth) pt V.
14 Ibid s 33D.
15 Ibid s 80W.
16 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Premier and Cabinet Circular No 12* (SA); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic). The *Privacy Act 1988* (Cth) has application to agencies in the Australian Capital Territory.

organisations that are exempt from the application of all of these Acts and whose activities may have an impact on individual privacy. These may include, for example, many small businesses.[17]

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

Health information privacy

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

3.15 Several state and territory laws also offer protections, including limitations on collection, use and disclosure, for health information held by state and territory public and private sector organisations.[21]

Communications privacy

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

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

---

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

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

19 *Healthcare Identifiers Act 2010* (Cth).

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

21 *Health Records and Information Privacy Act 2002* (NSW); *Information Privacy Act 2009* (Qld); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT); *Information Act* (NT).

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

23 Ibid s 276(3).

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

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

26 Ibid s 180F.

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

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

Surveillance laws and laws affecting photography

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

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

3.22 Different state and territory workplace surveillance legislation prohibits employers monitoring their employees at work through covert surveillance methods such as the use of CCTV cameras or computer, internet and email surveillance.[35] Once again there are inconsistencies between these laws, and such laws only exist in three jurisdictions (the ACT, NSW and Victoria).

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

---

27 Ibid s 108.
28 Ibid ss 110–132.
29 Ibid s 116(2).
30 Ibid s 7.
31 Ibid ss 9–18, 34–61A.
32 Ibid ss 46(2), 46A(2).
33 *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).
34 See Ch 13.
35 *Workplace Surveillance Act 2005* (NSW); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic); *Surveillance Devices Act 1998* (WA); *Workplace Privacy Act 2011* (ACT).
36 *Summary Offences Act 1988* (NSW) s 4; *Criminal Code Act 1899* (Qld) s 227(1); *Police Offences Act 1935* (Tas) s 13.

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

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

Harassment and stalking offences

3.25 State and territory laws criminalising harassment and stalking vary considerably depending on the jurisdiction. Legislation in Queensland and Victoria expressly prohibits 'cyber-harassment' committed through 'electronic messages'[41] or by 'otherwise contacting the victim'.[42]

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

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

Industry codes and guidelines

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

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

---

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

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

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

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

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

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

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

44 Ibid s 474.15.

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

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

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

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

Existing common law causes of action

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

Physical intrusions

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

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

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

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

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

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

Surveillance from outside a property

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

Intrusions into airspace

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Defamatory publications

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

---

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

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

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

63 Civil Aviation Safety Authority, *Submission 2*.

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

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

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

Disclosures of confidential information

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

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

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

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

Unauthorised photography

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

---

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

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

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

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

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

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

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

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

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

Gaps in existing law

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

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

---

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

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

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

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

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

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

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

---

79 A number of US states have enacted cyber-stalking or cyber-harassment legislation or have laws that explicitly include electronic forms of communication within more traditional stalking or harassment laws. Most of these constitute amendments to State Criminal Codes, updating the meaning of harassment and/or stalking to include electronic communications. In Nova Scotia in Canada, the *Cyber-Safety Act 2013* (SNS), c2 criminalises cyber-bullying.

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

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

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

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

A common law action for breach of privacy in Australia?

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

3.58 In *Sands v State of South Australia*, Kelly J stated that 'the *ratio decidendi* of the decision in *Lenah* is that it would require a further development in the law to acknowledge the existence of a tort of privacy in Australia'.[95]

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

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

---

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