14. Surveillance Devices

Contents

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*.