13. Surveillance Devices

Contents

Summary 195
Uniform surveillance laws 196
A technology-neutral definition of 'surveillance device' 198
Drones and mobile surveillance devices 199
Wearable devices 199
Data surveillance devices 200
Tracking devices 200
Uniform offences 201
Uniform defences and exceptions 202
Uniform workplace surveillance laws 205
Compensation for victims of surveillance 206
Surveillance device regulation by local councils 208
Civil penalties and interaction with the statutory cause of action 209

Summary

13.1 In this chapter, the ALRC proposes that surveillance device laws and workplace surveillance laws should be made uniform throughout Australia.

13.2 Existing surveillance device laws in each state and territory provide criminal offences for the unauthorised use of listening devices, optical surveillance devices, tracking devices, and data surveillance devices. These surveillance device laws provide important privacy protection by creating offences for unauthorised surveillance.

13.3 However, there is significant inconsistency between the laws with respect to the types of devices regulated and with respect to the offences, defences and exceptions. This inconsistency results in reduced privacy protections for individuals, and increased uncertainty and compliance burdens for organisations.

13.4 Additionally, the ALRC proposes that surveillance device laws make provision for courts to award compensation to victims of breaches of surveillance device laws. The ALRC has also asked whether local councils should be empowered to regulate the use of surveillance devices in some circumstances. Council regulation may be more appropriate for less serious uses of surveillance devices.

Uniform surveillance laws

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

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

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

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

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

13.5 Surveillance device laws provide an important protection of privacy. Notably, the legislation offers some protection against intrusion into seclusion. Consistency in these laws is important both for protecting individuals' privacy and for reducing the compliance burden on organisations that use surveillance devices in multiple jurisdictions.

13.6 Protection from surveillance is a fundamental form of protection of privacy, particularly in the digital era. One US judge has described the impact of surveillance on privacy:

> What the ancients knew as 'eavesdropping' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb. Electronic surveillance is the greatest leveller of human privacy ever known.[1]

13.7 Surveillance laws protect other freedoms as well. Unauthorised surveillance may interfere with freedom of speech, freedom of movement and freedom of association.

13.8 Laws exist in each state and territory to regulate the use of surveillance devices.[2] These laws provide criminal offences for the unauthorised installation, use or

---

1 Douglas J of the Supreme Court (United States of America) as cited in *Miller v TCN Channel Nine* (1988) 36 Crim R 92, 94 (Finlay J).

2 *Surveillance Devices Act 2007* (NSW); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act* (NT). At the Commonwealth level, the *Surveillance Devices Act 2004* (Cth) makes provisions for the use of

maintenance of surveillance devices to record private conversations and private activities.[3] Other laws in the ACT, NSW and Victoria regulate the use of surveillance in the workplace.

13.9 These surveillance device and workplace surveillance laws contain a number of significant inconsistencies across jurisdictions. These inconsistencies fall broadly into three categories. There are inconsistencies with respect to:

- the type of the devices regulated;
- the nature of the offences; and
- the nature of the defences and exceptions.

13.10 Consistency and uniformity in the surveillance device laws and workplace surveillance laws is desirable. Inconsistency means that privacy protections vary depending on which state or territory a person is located in. It also makes it more difficult for a person who finds themselves under surveillance to determine their legal position. Inconsistency also means that organisations with legitimate uses for surveillance devices face increased uncertainty and regulatory burden. Many stakeholders agreed that uniformity was desirable.[4] The ALRC discussed the benefits of uniformity in its 2008 report, 'For your information: Australian privacy law and practice'.[5]

13.11 The ALRC has proposed that definitions, offences, prohibitions, defences and exceptions be made uniform across Australian states and territories. This proposal applies both to surveillance device laws and to workplace surveillance laws.

13.12 The ALRC has not proposed a particular process for achieving uniformity. It may be appropriate for the Commonwealth to introduce new legislation, possibly through the introduction of a Commonwealth Act that covers the field, replacing state and territory surveillance device laws. Any such Commonwealth legislation would likely engage the external affairs power of the Australian *Constitution*, as a means of giving effect to Australia's obligation under art 17 of the *International Covenant on Civil and Political Rights* to protect privacy.[6] Alternatively, a new Act may be supported by s 51(v) if it is characterised as regulating 'postal, telegraphic, telephonic,

---

surveillance devices by federal law enforcement officers, however it does not provide for offences applicable to general members of the public.

3 Other laws provide related protections, without necessarily being designed to control the use of surveillance devices per se. For example, s 227A of the Queensland *Criminal Code* provides for a misdemeanour where a person observes or visually records another person 'in circumstances where a reasonable adult would expect to be afforded privacy', if the second person is in a private place or engaged in a private act and has not provided consent. A similar offence exists in s 91K of the *Crimes Act 1900* (NSW), where the recording is obtained for the purpose of obtaining 'sexual arousal or sexual gratification'. While a surveillance device could be used in a way that contravened one of these laws, surveillance may occur in other situations. Surveillance is also included as a form of stalking in, eg, s 21A(f) of the *Crimes Act 1958* (Vic).

4 M Paterson, *Submission 60*; Free TV, *Submission 55*; Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; Australian Industry Group, *Submission 38*; Law Institute of Victoria, *Submission 22*; D Butler, *Submission 10*.

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) ch 3.

6 The external affairs power and the ICCPR are discussed further in Ch 4.

and other like services'. A Commonwealth Act that covered the field would exist alongside other Commonwealth privacy protections under the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth). The ALRC has asked whether it would be preferable to enact a Commonwealth law to replace state and territory surveillance device laws, rather than attempting to achieve uniformity in state and territory laws.

A technology-neutral definition of 'surveillance device'

13.13 Uniform surveillance device laws should adopt a technology-neutral definition of 'surveillance device' to ensure that the definition can be applied to a wide range of surveillance devices, including surveillance devices that emerge in the future. The definition should also extend to forms of surveillance that are not 'devices', such as data surveillance by software installed on a person's computer.[7]

13.14 This element of the ALRC's proposal would address the inconsistencies in the types of devices regulated under the existing surveillance device laws. Four types of devices are recognised in at least one surveillance device law: listening devices, optical surveillance devices, data surveillance devices and tracking devices. However:

- optical surveillance devices are not regulated by the surveillance device laws of the ACT, Queensland, SA or Tasmania;
- data surveillance devices are not regulated by the surveillance device laws of the ACT, Queensland, SA, Tasmania, or WA, and are only regulated by the Victorian and NT surveillance device laws when used, installed or maintained by law enforcement officers; and
- tracking devices are not regulated by the surveillance device laws of the ACT, Queensland, SA, or Tasmania.

13.15 Even where two jurisdictions regulate similar devices, there are some inconsistencies in the definition of those devices.

13.16 In NSW, for instance, a tracking device is defined as 'any electronic device capable of being used to determine or monitor the geographical location of a person or an object',[8] while in Victoria, the definition is 'an electronic device the primary purpose of which is to determine the geographical location of a person or an object'.[9] Many general-purpose devices—in particular, mobile phones—can also be used to determine location, despite this not being the primary purpose of the device. This difference in definition may therefore have a significant impact on the types of surveillance that are regulated in each state.

13.17 In a 2001 interim report, the NSWLRC proposed defining 'surveillance device' as 'any instrument, apparatus or equipment used either alone, or in conjunction with

---

7 *R v Gittany (No 5)* [2014] NSWSC 49 (11 February 2014) [7].
8 *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of 'tracking device').
9 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'tracking device').

other equipment, which is being used to conduct surveillance'.[10] The NSWLRC also proposed defining 'surveillance' as 'the use of a surveillance device in circumstances where there is a deliberate intention to monitor a person, a group of people, a place or an object for the purpose of obtaining information about a person who is the subject of the surveillance'.[11]

13.18 The regulation of several types of surveillance devices are discussed below. The ALRC welcomes comments from stakeholders on the appropriateness of regulating these or other types of surveillance devices.

Drones and mobile surveillance devices

13.19 The use of unmanned aerial vehicles (drones) to carry surveillance devices has generated some concern within Australia and internationally.[12] Although a drone by itself may not be a surveillance device, other devices attached to a drone (such as microphones or video cameras) may be.

13.20 The OAIC noted community concerns about drones in its 2012–13 annual report.[13] At the time of writing, the House of Representatives Standing Committee on Social Policy and Legal Affairs is conducting an inquiry into the use of drones.[14]

13.21 The ALRC has also received a number of submissions relating to drones. Some stakeholders noted, in general terms, the privacy issues relating to the use of drones.[15] Others commented on the use of drones to monitor activity taking place on farms.[16]

Wearable devices

13.22 Wearable devices, such as head-mounted cameras, have also generated public discussion. A notable example is Google's 'Glass' technology, a wearable device that includes video and audio recording capabilities. Several stakeholders noted the privacy challenges presented by such devices.[17]

13.23 Wearable devices with audio recording capabilities would typically fall within the definition of 'listening device' in each of the surveillance device laws. Similarly, wearable devices with optical recording capabilities would typically fall within the

---

10 NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) Rec 1.
11 Ibid Rec 2.
12 See, for example, 'Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft' (American Civil Liberties Union, December 2011).
13 Office of the Australian Information Commissioner, *Annual Report* (2012), xv.
14 House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, Inquiry into a matter arising from the 2012-13 Annual Report of the Office of the Australian Information Commissioner, namely the regulation of Unmanned Aerial Vehicles (2013).
15 Electronic Frontiers Australia, *Submission 44*; Arts Law Centre of Australia, *Submission 43*; Australian Privacy Foundation, *Submission 39*; Office of the Information Commissioner, Queensland, *Submission 20*.
16 Barristers Animal Welfare Panel and Voiceless, *Submission 64*; National Farmers' Federation, *Submission 62*; RSPCA, *Submission 49*; Australian Lot Feeders' Association, *Submission 14*.
17 Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*; D Butler, *Submission 10*; P Wragg, *Submission 4*.

definition of 'optical surveillance device' in those laws that contain such a definition. However, several jurisdictions do not regulate optical surveillance devices.

13.24 It is important to note that uniform surveillance device laws would not, and should not, prohibit the use of such devices generally. A wearable device may have many legitimate uses that do not amount to surveillance. Whether or not the use of a device constituted an offence would depend on the circumstances of its use, such as the activity being captured, the extent of the monitoring or recording, and whether or not parties to the activity were aware that the device was being used.

Data surveillance devices

13.25 Surveillance device laws generally do not regulate phone tapping and other types of data or communications surveillance. Communications surveillance is regulated under the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act). Although the distinction between the two types of surveillance may become less clear as communication technologies continue to develop, the High Court has established that the TIA Act 'covers the field' of communications surveillance.[18]

13.26 Some surveillance device laws regulate some types of data surveillance—for example, devices that capture data by recording a person's keystrokes on a computer.[19] Other types of data surveillance may not be regulated under either surveillance device laws or the TIA Act. For example, information being transmitted over a radiocommunication system such as a wireless local network (wi-fi) appears to be excluded from the protections of the TIA Act[20] and may also fall outside existing definitions of 'data surveillance device'. Also, as noted in a submission from Associate Professor Moira Paterson,[21] radio frequency identification (RFID) devices such as electronic door key cards or passports are capable of transmitting information, and should also be protected from surveillance.

13.27 These types of data surveillance would need to be considered in drafting new uniform surveillance device laws.

Tracking devices

13.28 At present, tracking devices are regulated in only a few Australian jurisdictions. The definition of 'tracking device' is not consistent among these jurisdictions. Uniform surveillance device laws should address this inconsistency and ensure that tracking devices are regulated across Australia.

13.29 Consideration should also be given to regulating methods of tracking that do not rely on a tracking device being carried by the individual, but instead make use of a network of devices to determine the individual's location.[22] This could include, for

---

18 *Miller v Miller* (1978) 141 CLR 269.

19 See, eg, *Surveillance Devices Act* (NT) s 4 (definition of 'data surveillance device').

20 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5 (definitions of 'telecommunications network' and 'telecommunications service').

21 M Paterson, *Submission 60*.

22 Ibid; Electronic Frontiers Australia, *Submission 44*.

example, a communications network being used to determine the location of an individual's mobile phone, even where the mobile phone does not provide location information directly.[23]

Uniform offences

13.30 The ALRC proposes establishing uniform offences for the use of surveillance devices to monitor 'private activities' (however defined). The protection of privacy of individuals within Australia should not depend on the state or territory where the individual is located. One important step towards achieving uniformity would be ensuring that a given activity receives the same protection from surveillance regardless of the jurisdiction in which it occurs. To that end, a uniform definition of 'private activity' could be adopted.[24] This would be in keeping with the largely uniform definitions of 'private conversation' that apply in each jurisdiction for the purposes of the offence for surveillance using a listening device.

13.31 Each of the surveillance device laws provides a number of offences. These offences include, for example, offences for carrying out surveillance, offences for communicating information obtained by surveillance,[25] and offences for providing surveillance devices for sale.[26]

13.32 This chapter is concerned with the first of these types of offence—offences for carrying out surveillance.[27] The nature of these surveillance offences under existing surveillance device laws differ across jurisdictions. Each jurisdiction has an offence of carrying out surveillance of a private conversation using a listening device.[28] However, the offences with respect to other types of devices are inconsistent. For example:

- the offence for optical surveillance of a private activity in Victoria does not apply to activities carried on outside a building—optical surveillance of activities in a person back yard, for example, are permitted under the Victorian Act;[29]

---

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

24 An alternative approach would be to follow the NSW Act and define the offences in terms of interference with property rather than by reference to the nature of the conversation or activity under surveillance: *Surveillance Devices Act 2007* (NSW) s 8.

25 Eg, *Surveillance Devices Act 1999* (Vic) ss 11, 12; *Surveillance Devices Act* (NT) ss 15, 16.

26 *Surveillance Devices Act 2007* (NSW) s 13.

27 This is not to say that there are no inconsistencies in the other types of offences. However, the offences for carrying out surveillance are the primary protections of privacy in these laws, and so removing the inconsistencies in these offences is a priority.

28 Eg, *Surveillance Devices Act 1998* (WA) s 5; *Listening and Surveillance Devices Act 1972* (SA) s 4; *Invasion of Privacy Act 1971* (Qld) s 43.

29 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'private activity'). The Victorian Law Reform Commission has previously recommended removing the exception for activities carried on outside a building; see Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 11.

- the offences for optical and data surveillance in NSW do not depend on the nature of the activity or information placed under surveillance, but only on whether the installation, use or maintenance of the surveillance device required entry onto premises or interference with a car, computer or other object;[30] and
- the offences for data surveillance in Victoria and the NT provide a more general offence for using a data surveillance device to monitor information input to, or output from, a computer system, but these offences only apply to law enforcement officers.[31]

13.33 Differences also exist between the surveillance device laws with respect to the fault element in the offences for installing, using or maintaining a surveillance device. For example:

- the offence for the use of a listening device under the *Listening and Surveillance Devices Act 1972* (SA) requires intentional use of the device;[32]
- the offence for the use of a listening device under the *Invasion of Privacy Act 1971* (Qld) does not require intent,[33] although an exception applies for the 'unintentional hearing of a private conversation by means of a telephone';[34] and
- the offence for the use of a listening device under the *Listening Devices Act 1991* (Tas) includes an exception for 'the unintentional hearing of a private conversation by means of a listening device'[35]—not just for unintentional hearing by means of a telephone, as in the Queensland law.

13.34 There are other inconsistencies in the surveillance device laws with regard to other offences, such as the communication of information obtained through prohibited surveillance. In order to ensure uniformity between the surveillance device laws, such inconsistencies would need to be removed as well. However, these other offences are largely dependent on the general offences (for installing, using, or maintaining surveillance devices) considered above. Achieving uniformity in these more general offences is therefore a prerequisite for obtaining uniformity in the remaining offences.

Uniform defences and exceptions

13.35 As well as uniform offences, the surveillance device laws of each state and territory should, as far as possible, provide for uniform defences and exceptions.[36]

13.36 Many state and territory surveillance device laws contain a number of broadly similar exceptions to the offence of using, installing or maintaining a surveillance device. All jurisdictions permit surveillance in accordance with a warrant or other

30 *Surveillance Devices Act 2007* (NSW) ss 8, 10.
31 *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9.
32 *Listening and Surveillance Devices Act 1972* (SA) s 4.
33 *Invasion of Privacy Act 1971* (Qld) s 43(1).
34 Ibid s 43(2)(b).
35 *Listening Devices Act 1991* (Tas) s 5(2)(d).
36 The inconsistency of defences in existing surveillance device laws was noted by D Butler, *Submission 10*.

authorisation,[37] and all jurisdictions permit surveillance of a private conversation or activity if all the parties to the conversation or activity provide consent. Exceptions also exist for surveillance carried out in accordance with other legal requirements.[38]

13.37 One significant difference between the surveillance device laws relates to surveillance of a private conversation or activity by a party to that conversation or activity. Typically, an exception to a surveillance offence exists where all parties to the private conversation or activity provide consent.[39] However, in several jurisdictions, consent is not required if the person using, installing or maintaining the surveillance device is a party to the private activity or private conversation.[40]

13.38 The inconsistency with regard to this exception for participants means, for instance, that a journalist who records a conversation to which they are a party may have committed an offence in one jurisdiction, while the same recording would be permitted in another jurisdiction. The VLRC has referred to this exception for participants as a 'participant monitoring exception'.[41]

13.39 Other defences and exceptions also differ between jurisdictions:

- some jurisdictions provide an exception if the surveillance has the consent of all 'principal parties' to a conversation, being those parties that speak or are spoken to in a private conversation or who take part in a private activity;[42]
- some jurisdictions provide an exception if the surveillance has the consent of one principal party to a conversation and is reasonably necessary for the protection of a lawful interest of that principal party;[43]
- some jurisdictions provide an exception if the surveillance has the consent of one principal party and is not carried out for the purpose of communicating the

---

37 *Surveillance Devices Act 2007* (NSW) ss 7(2)(a), 8(2)(a), 9(2)(a), 10(2)(a); *Invasion of Privacy Act 1971* (Qld) s 43(2)(c); *Listening and Surveillance Devices Act 1972* (SA) s 6; *Listening Devices Act 1991* (Tas) s 5(2)(a); *Surveillance Devices Act 1999* (Vic) ss 6(2)(a), 7(2)(a), 8(2)(a), 9(2)(a); *Surveillance Devices Act 1998* (WA) ss 5(2)(a), 5(2)(b), 6(2)(a), 6(2)(b), 7(2)(b), 7(2)(c); *Listening Devices Act 1992* (ACT) s 4(2)(a); *Surveillance Devices Act* (NT) ss 11(2)(a), 12(2)(a), 13(2)(a), 14(2)(a).

38 Such requirements can be found, for example, in *Liquor Regulation 2008* (NSW) r 53H; *Transport (Taxi-Cab) Regulations 2005* (Vic) r 15.

39 See, for example, *Surveillance Devices Act 2007* (NSW) s 7(3); *Listening and Surveillance Devices Act 1972* (SA) s 4; *Surveillance Devices Act 1998* (WA) ss 5(3), 6(3). In some jurisdictions, it is sufficient that the 'principal parties' to the conversation or activity provide consent.

40 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1); *Invasion of Privacy Act 1971* (Qld) s 43(2)(a); *Surveillance Devices Act* (NT) ss 11(1)(a), 12(1)(a).

41 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) [6.54]–[6.58].

42 *Listening Devices Act 1992* (ACT) s 4(3)(a); *Surveillance Devices Act 2007* (NSW) s 7(3)(a); *Listening Devices Act 1991* (Tas) s 5(3)(a); *Surveillance Devices Act 1998* (WA) ss 5(3)(c), 6(3)(a).

43 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening and Surveillance Devices Act 1972* (SA) s 7(1) (but note that this does not require that the person is a principal party, merely a party); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii).

recording, or a report of the recording, to anyone who was not a party to the conversation or activity;[44] and

- some jurisdictions provide an exception where the use of a surveillance device is in the public interest.[45]

13.40 The ALRC proposes that the defences and exceptions in the surveillance device laws be made consistent. In removing inconsistencies, it is necessary to decide which defences and exceptions should remain. The ABC expressed a concern that uniformity might be achieved by removing important defences and exceptions that allow for the use of surveillance devices in the public interest.[46] The ALRC has specifically proposed a defence for responsible journalism (discussed further below).

13.41 The ALRC also proposes that unified surveillance device laws do not include a participant monitoring exception. Removing this exception would provide greater privacy protections to individuals. Removing the exception would also provide greater freedom of expression to individuals, who would be able to take part in conversations and activities confident that no other participant was recording the event.

13.42 The VLRC similarly proposed removing the participant monitoring exception from the *Surveillance Device Law 1999* (Vic),[47] noting that:

> [i]t is strongly arguable that it is offensive in most circumstances to record a private conversation or activity to which a person is a party without informing the other participants.[48]

13.43 In the absence of the participant monitoring exceptions, certain other exceptions or defences may be appropriate. An exception may be appropriate where a person using surveillance is a party to a conversation or activity and the use of the surveillance is necessary for the protection of a lawful interest of that person. As noted earlier, this exception exists in other surveillance device laws,[49] but is redundant where a participant monitoring exception applies.

13.44 An exception should continue to apply where the consent of all parties had been obtained. Legitimate uses of surveillance devices (for example, to record a consumer's agreement to the terms of a contract over the phone) would therefore not be affected, provided consent was obtained.

---

44 *Listening Devices Act 1992* (ACT) s 4(3)(b)(ii); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(ii) (this exception is not available with respect to optical surveillance); *Listening Devices Act 1991* (Tas) s 5(3)(b)(ii).

45 *Surveillance Devices Act 1998* (WA) s 24 (definition of 'public interest'); *Surveillance Devices Act* (NT) s 41 (definition of 'public interest').

46 ABC, *Submission 46*.

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

48 Ibid [6.57].

49 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening and Surveillance Devices Act 1972* (SA) s 7(1) (but note that this does not require that the person is a principal party, merely a party); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii).

13.45 Some legitimate uses of surveillance devices by journalists may place journalists at risk of committing an offence under existing surveillance device laws. Responsible journalism is an important public interest and should be protected. Journalists and media organisations should not be placed at risk of committing a criminal offence in carrying out legitimate journalistic activities. The ALRC has therefore proposed a 'responsible journalism' defence to surveillance device laws. This defence should be confined to responsible journalism involving the investigation of matters of public concern and importance, such as the exposure of corruption.

13.46 A number of other exceptions, as noted above, are already present in a number of the surveillance device laws. These exceptions should be considered in any process to make the surveillance device laws uniform.

Uniform workplace surveillance laws

13.47 Workplace surveillance legislation is also inconsistent across jurisdictions. Workplace surveillance laws recognise that employers are justified in monitoring workplaces for the purposes of protecting property, monitoring employee performance or ensuring employee health and safety. However, the interests of employers must be balanced against employees' reasonable expectations of privacy in the workplace. Specific workplace surveillance laws (the workplace surveillance laws) exist only in NSW,[50] the ACT[51] and, to some extent, in Victoria.[52] As with general surveillance device laws, uniformity about workplace surveillance laws would promote certainty, particularly for employers and employees located in multiple jurisdictions.

13.48 The *Surveillance Devices Act 1999* (Vic) provides an offence for the use of an optical device or listening device to carry out surveillance of the conversations or activities of workers in workplace toilets, washrooms, change rooms or lactation rooms.[53] Workplace surveillance in Victoria is otherwise subject to the same restrictions as general surveillance devices.

13.49 The *Workplace Privacy Act 2011* (ACT) applies to optical devices, tracking devices and data surveillance devices, but not to listening devices.[54] The Act requires an employer to provide particular forms of notice to employees if one of these types of surveillance devices is in use in the workplace, and to consult with employees in good faith before surveillance is introduced.[55] The Act also provides for 'covert surveillance authorities', allowing an employer to conduct surveillance without providing notice upon receiving an authority from a court. A covert surveillance authority will be issued only for the purpose of determining whether an employee is carrying out an unlawful activity, and is subject to various safeguards.[56] The ACT Act also prohibits

50 *Workplace Surveillance Act 2005* (NSW).
51 *Workplace Privacy Act 2011* (ACT).
52 *Surveillance Devices Act 1999* (Vic) pt 2A.
53 Ibid s 9B.
54 *Workplace Privacy Act 2011* (ACT) s 11(1) (definition of 'surveillance device').
55 Ibid pt 3.
56 Ibid pt 4.

surveillance of employees in places such as toilets, change rooms, nursing rooms, first-aid rooms and prayer rooms, and surveillance of employees outside the workplace.[57]

13.50 The *Workplace Surveillance Act 2005* (NSW) similarly applies only to 'optical surveillance', 'computer surveillance' and 'tracking surveillance'.[58] The NSW Act contains similar restrictions to those under the ACT Act. Surveillance devices must not be used in a workplace without sufficient notice being provided to employees,[59] must not be used in a change room, toilet, or shower facility,[60] and must not be used to conduct surveillance of the employee outside work.[61] Covert surveillance must not be used unless a covert surveillance authority is obtained.[62] The NSW Act also places limitations on the restriction of employee email and internet access while at work.[63]

13.51 The inconsistencies between these workplace surveillance laws are relatively minor—for example, slightly different definitions apply, and the types of rooms that may not be put under surveillance differ slightly between each law. A more significant need for reform arises because specific workplace surveillance laws exist only in these jurisdictions. The ALRC therefore proposes that there be uniform workplace surveillance laws across Australia.

13.52 Establishing uniform workplace surveillance laws in each of the states and territories would provide greater privacy protections for employees and greater certainty for employers operating in multiple jurisdictions. These laws could be contained in specific workplace surveillance laws, as they are in the ACT and NSW, or integrated into the more general surveillance device laws, as they are in Victoria.[64]

Compensation for victims of surveillance

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

13.53 Privacy protections afforded to individuals by the criminal law are limited in that the criminal law punishes the offender without necessarily providing redress to the

57 Ibid pt 5.

58 *Workplace Surveillance Act 2005* (NSW) s 3. The definition of 'tracking surveillance' refers to a device 'the primary purpose of which is to monitor or record geographical location or movement'. This is arguably another inconsistency in surveillance laws. The definition of 'tracking device' in s 4 of the *Surveillance Devices Act 2007* (NSW) does not require that tracking be the primary purpose of the device, but the definition of 'tracking device' in s 3 of the *Workplace Surveillance Act 2005* (NSW) does require that tracking be the primary purpose.

59 Ibid pt 2.

60 Ibid s 15.

61 Ibid s 16. An exception applies where the surveillance is computer surveillance on equipment provided at the employer's expense.

62 Ibid pt 4.

63 Ibid s 17.

64 The latter, integrated approach was recommended by the NSWLRC: NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001) Rec 57.

victim. While an individual who has been subjected to unlawful surveillance may gain some satisfaction from seeing the offender fined, and while the fine may dissuade the offender from conducting further unlawful surveillance in the future, the victim will generally not receive any compensation or other personal remedy.

13.54 If uniform surveillance device laws are introduced through reforms to existing state and territory legislation, a provision allowing for compensation to victims would operate alongside compensation provisions already provided for by existing state and territory legislation.[65] However, providing for compensation within the uniform surveillance device laws would ensure that uniform compensation mechanisms existed for victims of unlawful surveillance.

13.55 All states and territories have established victims' compensation schemes that provide for compensation to be paid to victims of crimes.[66] Unlike an order for compensation to be paid by an offender, a victims' compensation scheme does not depend on an offender's ability to pay the compensation. However, victims' compensation schemes are generally available only for serious physical crimes such as assault, robbery, or sexual assault,[67] and surveillance is therefore unlikely to give rise to compensation under these schemes.

13.56 The ALRC proposes that the surveillance device laws of the states and territories—whether made uniform or not—should allow courts to order compensation be paid to individuals who are victims of unlawful surveillance. Such a change to surveillance device laws was suggested by Professor Des Butler, who submitted that the laws 'should in addition make provision for recovery of compensation or other remedies such as injunction by any aggrieved person'.[68]

13.57 Mechanisms for compensation can be found in other, analogous, criminal laws. Remedial relief is available, for example, under s 107A of the *Telecommunications (Interception and Access) Act 1997* (Cth). Under this section, an aggrieved individual may apply to the court for remedial relief if a defendant is convicted of intercepting or communicating the contents of a communication.[69]

---

65 Courts may order compensation for loss, injury or damage under, for example, *Crimes (Sentencing) Act 2005* (ACT) s 18; *Criminal Law (Sentencing) Act 1988* (SA) s 53; *Sentencing Act 1991* (Vic) s 85B; *Victims Rights and Support Act 2013* (NSW) ss 91–103.

66 For a general discussion of these schemes, see Australian Law Reform Commission and NSW Law Reform Commission, *Family Violence: A National Legal Response*, ALRC Report No 114, NSWLRC Report 128 (October 2010) ch 4.

67 *Victims Rights and Support Act 2013* (NSW) s 5; *Victims of Crime Assistance Act 1996* (Vic) ss 7–13.

68 D Butler, *Submission 10*.

69 The remedies available under this section include, but are not limited to: a declaration that the interception or communication was unlawful; an order for payment of damages; an order, similar to or including, an injunction; and an order that the defendant pay the aggrieved person an amount not exceeding any income derived by the defendant as a result of the interception or communication: *Telecommunications (Interception and Access) Act 1979* (Cth) s 107A(7).

Surveillance device regulation by local councils

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

13.58 A number of submissions have raised concerns regarding CCTV cameras, installed for security in homes and offices, but that may also record the activities of neighbours. Such uses of surveillance may be more appropriately regulated by local councils, rather than surveillance device laws.

13.59 By regulating surveillance devices at the local council level, it may be possible to resolve many disputes without recourse to the criminal law. A clear and transparent resolution process via local council would also potentially increase access to justice in circumstances where criminal penalties may be perceived as too severe.

13.60 Local governments are responsible for duties such as assessing and authorising development of houses, granting or disallowing various structural changes to property and protection of the environment. In New South Wales, for example, the *Environmental Planning and Assessment Act 1979* (NSW) and related planning instruments set out the types of development that require development consent from the local council. The installation of surveillance devices that overlook neighbouring properties could similarly require development consent.

13.61 Alternatively, the installation of surveillance devices could be included as a type of development that does not require development consent, provided certain conditions are met.[70]

13.62 Some councils already regulate surveillance devices. The City of Sydney Council, for example, has made determinations in the past on details such as the installation location and types of camera that may be used.[71] However, not all councils have such requirements.

13.63 Mechanisms for challenging local council decisions already exist in all states. For example, in NSW, review of a council's decision by the NSW Land and Environment Court is available under s 82A of the *Environmental Planning and Assessment Act 1979* (NSW). In Victoria, the Victorian Civil and Administrative Tribunal (VCAT) can hear appeals against decisions of planning and development applications made by local councils.[72]

---

70 The *State Environment Planning Policy (Exempt and Complying Development Codes) 2008* (NSW) (the Policy) sets out a range of developments which do not require council development consent, as long as certain conditions are met. For example, cls 2.3 and 2.4 of the Policy provide that development consent is not required for a aerial or antenna that at least 900mm away from a lot boundary and no higher than 1.8m above the highest point of the building's roof (if roof-mounted).

71 See, for example, *Szann v Council of City of Sydney* [2012] NSWLEC 1168 (21 June 2012).

72 *Planning and Environment Act 1987* (Vic) ss 77–86.

Civil penalties and interaction with the statutory cause of action

13.64 Some stakeholders suggested that a civil penalties regime should be considered to either complement or replace the criminal regime that currently exists under the surveillance device laws.[73] These stakeholders suggested that a civil penalties regime would be useful in light of the low levels of enforcement under the existing criminal regime. The VLRC has also recommended the introduction of a civil penalties regime in the *Surveillance Devices Act 1999* (Vic).[74]

13.65 There may be benefits in introducing a civil penalties regime into the surveillance device laws. For certain matters, a civil penalties process, potentially managed by a non-judicial regulator, could be cheaper, faster, and less burdensome than a criminal proceeding, both on the complainant and on the respondent. Additionally, criminal penalties may be unnecessarily severe for uses of surveillance devices that do not result in serious harm to the individual.

13.66 However, the ALRC has not proposed a civil penalties regime. The ALRC's proposal to allow courts to award compensation to victims of unlawful surveillance would achieve many of the objectives of a civil penalties regime, without the need to create new bodies to hear civil disputes about surveillance. Furthermore, the introduction of a statutory cause of action for serious invasion of privacy would provide another means of redress for unlawful surveillance. The introduction of a civil penalties regime for surveillance may result in overlap, excessive complexity and regulatory burden if a statutory cause of action were also introduced.

---

73 Electronic Frontiers Australia, *Submission 44*; Australian Privacy Foundation, *Submission 39*.

74 Victorian Law Reform Commission, *Surveillance in Public Places*, Report 18 (2010) Rec 19.