Chapter 6

Modernising the Surveillance Devices Act

CONTENTS

108 Introduction
108 Background
108 Definitions
112 Prohibition of surveillance devices in toilets
112 Regulating tracking devices
117 Removing the participant monitoring exception
121 A civil penalty regime
122 A new offence for improper use of a surveillance device
125 Conclusion
INTRODUCTION

6.1 This chapter deals with those parts of the Surveillance Devices Act 1999 (Vic) (SDA) where the commission recommends change to deal with advances in technology and to modernise the way we regulate the use of surveillance devices.

BACKGROUND

6.2 The Victorian parliament first dealt with surveillance devices in 1969 when it introduced the Listening Devices Act 1969 (Vic), which prohibited the use of listening devices to record or monitor private conversations. That Act also included requirements for obtaining a warrant to undertake covert surveillance with a listening device and provided exemptions for police in specific circumstances.

6.3 In 1999 parliament responded to advances in technology and the more widespread use of surveillance by passing the SDA. This Act regulates the use of optical surveillance devices, tracking devices and data surveillance devices as well as listening devices. The SDA has been amended on a number of occasions since then. Major amendments include prohibiting surveillance of workers in toilets and change rooms,1 and establishing an oversight and monitoring role for the Special Investigations Monitor in relation to law enforcement use of surveillance.2

6.4 Surveillance technology has become increasingly sophisticated, affordable, concealable and unobtrusive. Its use is now commonplace. People are subject to surveillance every day when they use public transport, shop for groceries, attend sporting events and walk down city streets.3

6.5 Technology has also changed the way people use public places. Activities that many people would still consider private, such as personal telephone conversations, now regularly take place in public places on mobile phones.

6.6 To reflect these changes in behaviour, and to ensure that the law keeps pace with advances in technology, the commission recommends a number of changes to clarify, modernise and strengthen the SDA. These include amending some important definitions to reflect contemporary uses of surveillance devices, expressly prohibiting surveillance in toilets and change rooms, strengthening the prohibition on participant monitoring, introducing a new offence to prohibit particularly offensive uses of surveillance devices, and introducing a civil enforcement regime into the Act.

DEFINITIONS

PRIVATE ACTIVITY

6.7 The SDA prohibits a person from using a listening device to monitor4 a ‘private conversation’ to which they are not a party if not all the people in the conversation have given their consent.5 Similarly, the Act prohibits a person from using an optical surveillance device to monitor a ‘private activity’ to which they are not a party if not all the people conducting the activity have given their consent.6

6.8 Under the Act, a conversation or activity is ‘private’ if it occurs in circumstances that reasonably indicate the parties desire it to be heard or observed by themselves only, and when they may reasonably expect that they will not be heard or observed by someone else.7
Currently, the definitions of ‘private conversation’ and ‘private activity’ differ in relation to the physical location of the conversation or activity being monitored. Although an activity cannot be ‘private’ if it occurs outside a building, a conversation may be ‘private’ regardless of where it occurs. It is unlawful for a person to use a listening device to record a private conversation without consent, either indoors or outdoors. By contrast, although a person cannot use an optical surveillance device indoors to record a private activity without consent, there is no such prohibition on the use of an optical surveillance device outdoors. Consequently, the SDA offers no protection against highly intrusive visual surveillance in outdoor places.

During the parliamentary debates that accompanied the passage of the SDA a number of members referred to the lack of protection for private activities in outdoor places, such as beaches and backyards. This issue generates community interest from time to time, such as when the satellite images and photographs published by Google Street View, and used by some NSW and Victorian councils, attracted publicity.

Advances in technology have meant that these different provisions in the SDA for listening devices and optical surveillance devices produce illogical outcomes. For example, the prohibition on recording a private conversation that occurs outside a building without consent may be lawfully circumvented by the use of a video recorder used in conjunction with lip-reading technology or services. Further, using a video recorder with sound recording capacity to record a private occurrence outside a building could breach the listening device offence in section 6 of the SDA without breaching the optical surveillance device offence in section 7. This is because of the limited definition of ‘private activity’ in the SDA.

Surveillance device legislation in Western Australia and the Northern Territory prohibits (with exceptions) the use of an optical surveillance device to record a private activity. Neither jurisdiction makes a distinction between whether the activity occurs indoors or outdoors. As well as this, NSW legislation that regulates optical surveillance devices does not make a distinction between indoor and outdoor activities.

The commission believes the SDA should prohibit the use of an optical surveillance device to monitor private activities that occur outdoors as well as indoors. This change would ensure consistency in the regulation of surveillance devices and would bring Victorian surveillance device legislation in line with legislation in other Australian jurisdictions.

Most visual surveillance activities that occur outdoors would not be affected by the commission’s proposal. This is because the prohibition in section 7 of the SDA against the use of a visual surveillance device applies only to ‘private activities’. These are activities that people do not wish others to observe, and which are not carried out in circumstances where they ought to reasonably expect that someone else may observe it. There are, however, some ‘private activities’ that do occur outdoors and in public places. It should be unlawful for people to monitor these activities with a visual surveillance device.
Modernising the Surveillance Devices Act

**RECOMMENDATION**

11. The words ‘an activity carried on outside a building’ should be removed from the definition of ‘private activity’ in section 3 of the SDA so that it reads:

    private activity means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else.

**IMPLIED CONSENT**

6.15 The prohibitions in the SDA concerning the use of listening, optical, tracking or data surveillance devices do not apply if the surveillance user has the express or implied consent of the person being monitored.\(^{15}\) As the Act does not define ‘consent’ common law principles concerning the meaning of consent probably apply. For example, at common law, a person must have capacity for consent to be valid and that consent must be given freely and voluntarily.\(^{16}\)

6.16 The notion of consent—particularly implied consent—is sometimes difficult to characterise when dealing with many common surveillance practices in public places. If, for example, a retail outlet has a sign on the door stating that cameras are in use on the premises, does this mean that all customers give their implied consent to being filmed when they walk into the shop, including when they enter change rooms to try on clothing? Does this include people who might not have the capacity to give consent, or those who cannot read the sign? In some circumstances it may be inconvenient (or impossible) for a person to opt out of being subject to surveillance, and therefore any implied consent may not be truly voluntary.

6.17 In its Privacy Report the Australian Law Reform Commission (ALRC) discussed the difficulties raised by the concept of consent, noting, in relation to personal information:

    There is a pressing need for contextual guidance on consent. What is required to demonstrate that consent has been obtained is often highly dependant on the context in which personal information is collected, used or disclosed.\(^{17}\)

6.18 To address this, the ALRC recommended that the Office of the Privacy Commissioner ‘develop and publish further guidance about what is required of agencies and organisations to obtain an individual’s consent for the purposes of the Privacy Act’.\(^{18}\) In our Consultation Paper we asked stakeholders whether a regulator should develop guidelines to clarify the meaning of consent. Many submissions supported this proposition. However, of those that did not, Victoria Police said this was a matter for parliament and the judiciary,\(^{19}\) and the Victorian Privacy Commissioner said the meaning of consent should be defined in the SDA itself.\(^{20}\)

6.19 Submissions also noted the difficulties in defining ‘implied behaviour’. The St Kilda Legal Service noted that consent should not be implied when an individual has no reasonable choice about being in a particular place. The service noted that the most marginalised groups—for example, homeless people—have little choice in avoiding public place surveillance.\(^{21}\) The Victorian Privacy Commissioner noted that even implied consent should be free, revocable and fully informed.\(^{22}\)
6.20 From a commercial perspective Sensis (the information and advertising arm of Telstra) said the lawfulness of their location-based services relied on implied consent. When, for example, a mobile phone user is offered details of the location of the closest petrol station via text message, the service provider must identify the phone owner’s location in order to provide that information. By requesting the service has the phone owner consented to having their location tracked by the service provider? Sensis said the status quo, where implied consent is not defined, operates effectively and flexibly and does not require legislative amendment.23

6.21 The commission acknowledges that in many instances it makes little sense to suggest that people whose activities are monitored by surveillance equipment in public places have given actual consent to a ‘private activity’ or a ‘private conversation’ being monitored by an optical surveillance device or a listening device. Nevertheless, the notion of ‘implied consent’24 remains the most practical dividing line between behaviour that should be prohibited in a public place because it is highly intrusive, unannounced and undetectable, and behaviour that should be permitted because reasonable attempts have been made to alert members of the public to the fact that some form of intrusive surveillance is occurring.

6.22 Given the widespread use of surveillance devices in public places, it is important to encourage surveillance device users to give adequate notice of their activities when they engage in practices that may involve monitoring of a ‘private conversation’ or a ‘private activity’. The SDA should actively encourage the practice of giving adequate notice of surveillance, by signage or other means, in these circumstances. The SDA should be amended to direct courts, when deciding whether a person has given implied consent to conduct that would otherwise fall within sections 6–9 and 11–12 of the SDA, to consider whether the defendant should have given adequate notice of the surveillance activities and whether in fact that notice was given. Although common law principles concerning the meaning of implied consent would otherwise continue to apply, this change would encourage surveillance users to ensure they do not conduct highly intrusive public place surveillance without providing adequate notice of their activities.

6.23 In some instances it may be appropriate to make limited use of well-placed signs, perhaps containing an image of a camera, to give people adequate notice of the fact that a CCTV surveillance system is being used in a way that is particularly intrusive. The regulator will be well placed to advise people about how to strike a balance between reasonable notice, the cost of erecting signs and the unsightly impact of some notices.

**RECOMMENDATION**

12. The SDA should be amended so that courts are directed to consider whether a public place surveillance user has given adequate notice of their surveillance activities when considering whether a person has given ‘implied consent’ to any of the conduct that falls within sections 6–9 and 11–12 of the SDA.
Modernising the Surveillance Devices Act

PROHIBITION OF SURVEILLANCE DEVICES IN TOILETS

6.24 At present, the SDA prohibits use of an optical surveillance device to monitor ‘private activity’—defined in the Act as an activity where parties may reasonably expect that they may not be observed by someone else—without consent. The explanatory memorandum to the Act suggests that the prohibition extends to activities in toilet cubicles, shower areas and change rooms.25

6.25 There is, however, uncertainty about the reach of this prohibition because in some instances a person would reasonably expect to be seen by others when using communal facilities, such as in open showers and at urinals.26 Perhaps because of the uncertainty about the reach of the current law, some fitness centres have independently instituted policies to ban mobile telephones (which may have camera devices) in such areas.27 The Victorian Privacy Commissioner has queried whether the comment in the explanatory memorandum to the SDA is an accurate description of the terms of the Act:

While courts can take note of the explanatory memoranda to statutes, courts might be reluctant to impose criminal liability for conduct that does not clearly fall within the terms of the Surveillance Devices Act, as currently drafted. It may be better to state explicitly in the Surveillance Devices Act that private activities do occur in certain public places and that invading the privacy of persons in those places is prohibited, with serious penalties for breach.28

6.26 The commission is of the view that the SDA should be amended to include an express prohibition on the use of all optical surveillance devices in toilet areas, shower areas and change rooms. As with other prohibitions in the SDA, this prohibition would not apply to law enforcement officers acting under warrant.

6.27 A prohibition of this nature appears to be in keeping with public expectations that these are no go areas where all surveillance is regarded as unacceptable. This view was strongly expressed in submissions and consultations.29 Further, many international codes of practice and guidelines30 prohibit, or greatly restrict,31 surveillance in such areas.

6.28 This reform proposal reflects our recommendation in the Workplace Privacy report that employers should be prohibited from using optical surveillance and listening devices to monitor the activities of workers in toilets, change rooms, lactation rooms and bathrooms.32 The Victorian parliament adopted that proposal in 2006 by inserting section 9B into the SDA.

RECOMMENDATION

13. The SDA should be amended to expressly prohibit the use of an optical surveillance device or listening device to observe, listen to, record or monitor any activity in toilets, shower areas and change rooms which form a part of any public place. This prohibition should include a law enforcement exemption similar to that in section 9B(2) of the SDA.

REGULATING TRACKING DEVICES

6.29 The use of tracking devices is regulated far more strictly under the SDA than the use of optical surveillance or listening devices. It is unlawful to use a tracking device without the consent of the person being tracked, unless one of the law enforcement exceptions applies. In contrast, it is unlawful to use an optical surveillance or listening device only when monitoring a private activity or a private conversation without consent. Again, this is subject to the law enforcement exceptions.
6.30 This distinction reflects the serious privacy implications of tracking a person without their consent. These implications were discussed by the New Zealand Law Commission (NZLC), which recommended that tracking a person without their consent should be generally prohibited in New Zealand. The NZLC notes:

Covert tracking robs people of the ability to choose whether or not others know where they are at a particular time. It can reveal very private information: that a person visited an abortion clinic or a gay bar for example … In the most serious cases, being tracked may make people feel insecure, or may genuinely threaten their safety if it is done by a violent ex-partner, for example.33

6.31 Currently, not all tracking devices are regulated under the SDA. Although an optical or listening device is defined as ‘any device capable’ of being used to record a person’s voice or activity under the Act, a tracking device is defined as a device the primary purpose of which is to determine the geographical location of a person or an object.34 This means that a device that is capable of tracking, but is not primarily used for that purpose (such as a mobile phone with GPS capacity), is not a tracking device covered by the Act.

6.32 In our Consultation Paper we asked whether it was appropriate for the definition of ‘tracking device’ to be amended so it includes any electronic device capable of being used to determine the geographical location of a person or object. This change would mean that the definition of ‘tracking device’ is consistent with the definitions of other surveillance devices that are concerned with the capacity of a device rather than its primary purpose.

6.33 There was broad support for amending the definition of ‘tracking device’ in this way. Consultees raised concerns about the unregulated use of some tracking devices. For example, the Victorian Women’s Legal Service expressed concern about ‘stalkers’ using tracking devices with no protection for the person who is being stalked.35

6.34 Amending the definition of ‘tracking device’ would create consistency with NSW legislation. The Surveillance Devices Act 2007 (NSW) does not use the ‘primary purpose’ test. It defines a ‘tracking device’ as ‘any electronic device capable of being used to determine or monitor the geographical location of a person or an object’ (emphasis added).

6.35 The commission recommends that the definition of ‘tracking device’ in the SDA be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object. However, we also recognise that there are many legitimate and beneficial uses of tracking devices. The SDA currently includes the following exemptions:

- the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation
- the installation, use or maintenance of a tracking device in accordance with a detention order or supervision order or an interim order under the Serious Sex Offenders (Detention and Supervision) Act 2009 (Vic)
- the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth.36
6.36 The commission is of the view that these are appropriate and necessary exemptions, and should continue to apply. In addition, there are other legitimate uses of tracking devices that should be exempted from the general prohibition against the use of a tracking device without consent. These are discussed below.

**AUTOMATIC NUMBER PLATE RECOGNITION**

6.37 Automatic number plate recognition (ANPR) devices use pattern recognition software to automatically detect and read the licence plates of vehicles that pass the system’s cameras and match these against registration records on a database. ANPR identifies the time and date of the scan and the GPS location. When multiple ANPR devices are used together, they can track the movement of a vehicle.

6.38 ANPR technology is a classic example of ‘convergence’ of surveillance technologies, as it uses both optical surveillance (cameras) and tracking devices (GPS) in order to determine the location of a vehicle. The use of ANPR does not infringe the prohibition on the use of optical surveillance devices in the SDA, as optical surveillance is prohibited in relation to a private activity only. However, as the current and proposed prohibition on the use of tracking devices is not limited to ‘private activities’, the continued use of ANPR is relevant when considering the regulation of tracking devices.

6.39 A number of organisations in Victoria use ANPR technology. For example, in 2009 Victoria Police trialled the use of ANPR in police cars to record the details of passing vehicles and detect those that may be unregistered or stolen. It is also possible for police to search for persons of interest using this technology. ANPR is also used to assist in the collection of road tolls on private tollways in Melbourne, and VicRoads uses the technology with red-light and speeding cameras across Victoria. In addition, ANPR may be used by governments and private organisations for a number of applications, including controlling access to restricted areas, congestion taxes, monitoring freight movement and calculating fees for unattended car parks.

6.40 Government agencies in many countries use ANPR technology for road safety and law enforcement purposes. It is estimated that there are at least 10,000 ANPR cameras in operation in the UK. These cameras provide data about over 10 million number plates per day to a national database run on behalf of the Association of Chief Police Officers. The data are kept for two years and are used for a number of purposes, including evidence in criminal trials. Concerns have been raised about possible misuse of this information.

6.41 In its submission to the commission Victoria Police noted that the commission’s proposed changes to the definition of tracking device would have a significant impact on police operations, particularly their use of ANPR technology, which they believe does not currently fall within section 8 of the SDA. Victoria Police believes that it would be ‘administratively unworkable’ to require police to obtain a warrant each time they wish to use ANPR. Victoria Police also raised concerns about the impact on emergency services in the case of missing persons. In addition, it seems desirable that VicRoads and tollway operators be permitted to continue to use ANPR for road safety and tolling purposes.

6.42 In NSW, ANPR has been an integral part of the Safe-T-Cam traffic monitoring system since 1989. In addition, NSW Police trialled ANPR use in 2009. It appears that these activities fall outside of the general prohibition against the use of tracking devices in section 9 of the *Surveillance Devices Act 2007 (NSW)* because of the exception in section 9(2)(c) that extends to ‘the installation, use or maintenance of a tracking device for a lawful purpose’.
6.43 This exception to the prohibition against using a tracking device without consent is both vague and unnecessarily broad. There are better ways of ensuring that all relevant interests are taken into account when deciding whether technology of this nature should be used to track the movements of people who are acting lawfully, as well as those who are acting unlawfully. One way would be to allow specific law enforcement activities to be exempted by regulation from the general prohibition against using a tracking device without consent.

6.44 This process should ensure that there is appropriate oversight of any decision to provide a law enforcement exception to the general prohibition against using a tracking device without consent. It is highly likely that the government would seek advice from the Privacy Commissioner and the proposed new surveillance regulator before preparing a regulation. Any regulation would be subject to parliamentary scrutiny and disallowance under the relevant provisions of the Subordinate Legislation Act 1994 (Vic).

6.45 The use of ANPR technology should be carefully monitored because of its potential for capturing vast amounts of information about individuals who are behaving lawfully. ANPR was the subject of a study by the Queensland Parliamentary Travelsafe Committee, which released a report in September 2008. A number of submissions (including those by the federal and Victorian Privacy Commissioners) raised privacy concerns in relation to the technology, including the appropriateness of recording and retaining data of people not identified as having done something illegal, and the potential for ANPR to be used for unintended purposes, referred to as ‘function creep’.46

6.46 The Committee made a number of recommendations, including the installation of signs that inform motorists that their image may be recorded, and legislation that contains safeguards and controls governing the use of ANPR technology. The Queensland government has implemented a number of the recommendations, including amending signs, and has committed to consider the Committee’s other recommendations concerning legislation.47

6.47 The commission recommends that the proposed regulator should advise parliament regularly about the use of ANPR technology in Victoria, including whether the current regulatory controls are adequate.

MANAGEMENT AND CARE OF PATIENTS

6.48 Another issue that arises in relation to tracking devices is their use in the management and care of people suffering from dementia and other memory-affecting conditions. Alzheimer’s Australia recommends that carers consider the use of a GPS-enabled tracking device, such as a bracelet-type device, to monitor a person with dementia so that the individual can freely go for walks on their own but can be easily located if they are lost or disoriented.48 In many instances the person being tracked may not have the capacity to consent to being monitored by a device that enables them to be located.

6.49 It should be possible to use tracking devices to protect the health, safety and wellbeing of people in these circumstances. The New Zealand Law Commission has considered this issue in relation to its proposal that new surveillance legislation include a prohibition on the use of tracking devices. The Commission notes:

We think that it should be a defence to the tracking device offence that the use of the tracking device was necessary for the protection of the health, safety or wellbeing of any person, or for the protection of public health or safety, and was no more extensive than reasonably necessary for those purposes.49
Modernising the Surveillance Devices Act

6.50 The Commission notes the defence would cover such situations as:

- use of tracking devices to monitor the movements of dementia patients
- use of tracking devices by parents or guardians to monitor the location of their children
- use by hospital management to track the movements of patients within the hospital.

6.51 These defences may go too far. The family, friends and/or carers of people suffering from dementia and other memory-affecting conditions should be able to use a tracking device to locate that person if they are lost or disorientated. That person’s freedom of decision and action is enhanced by permitting them to move around the community as freely as possible so long as they do not pose a threat to their own safety or that of others. If the person is unable to consent to the use of the tracking device because of lack of capacity, there should be an automatic substitute consent-giving regime that is similar to that which applies to consent for medical treatment set out in Part 4A of the Guardianship and Administration Act 1986 (Vic).

6.52 The Guardianship and Administration Act 1986 (Vic) establishes a hierarchy of people, known as the ‘person responsible’, who may consent to most forms of medical treatment on behalf of a person who cannot consent to it themselves. These people range from a medical agent and guardian to a spouse or primary carer. This regime should be extended so that the ‘person responsible’ may consent to the wearing of a tracking device.

6.53 The issue of substituted consent for using a tracking device to monitor the location of a child is far more complex. Children of a certain age should be able to move freely around the community without parents tracking them, no matter how well meaning they may be. The proposed new regulator may choose to report to parliament about this issue.

RECOMMENDATION

14. The definition of ‘tracking device’ in section 3 the SDA should be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object.

15. The Governor in Council should be permitted to make regulations that allow specific law enforcement activities to be exempted from the general prohibition in section 8 of the SDA against using a tracking device without consent.

16. The proposed new regulator should advise parliament regularly about the use of ANPR technology in Victoria, including whether the current regulatory controls are adequate.

17. The automatic substitute consent regime in Part 4A of the Guardianship and Administration Act 1986 (Vic) should be extended so that the ‘person responsible’ may consent to the installation of a tracking device for a person over the age of 18 years who is incapable of giving consent to the installation of that device.
REMOVING THE PARTICIPANT MONITORING EXCEPTION

6.54 The SDA’s prohibition on recording a conversation or activity using a surveillance device applies only to people who are not a party to the conversation or activity. It does not prohibit a person from recording a private conversation or activity to which they are a party.52 This activity is known as ‘participant monitoring’.

6.55 At present it is quite lawful for one person to secretly record his or her conversation with another person on a park bench, or to secretly film an encounter with another on a secluded beach. These are places where it might be reasonable for a person to expect that a conversation or activity would not be overheard or seen by others.

6.56 Publication of information gained through participant monitoring is unlawful however. Section 11 of the SDA prohibits publication of a record or report of ‘private conversation’ or ‘private activity’ that has been made by using a surveillance device.53 There are a number of exceptions to this prohibition that are set out in section 11(2) of the SDA.

6.57 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.54 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. For example, the SDA currently permits a participant in a sexual act to record that activity without the knowledge and consent of the other party involved.55

6.58 Finally, as we noted in our Consultation Paper, most Australian states prohibit participant monitoring under their surveillance devices legislation.56 Only Queensland and the Northern Territory have similar participant monitoring exceptions to those in the Victorian legislation.57

ALLOWING SOME INSTANCES OF PARTICIPANT MONITORING

6.59 It is also arguable that some forms of participant monitoring are beneficial and should continue to be permitted. Participant monitoring allows individuals to protect their interests, particularly in ‘commercial, business and domestic contexts’.58 For example, the commission was told that participant monitoring is used by parties in domestic violence and family law matters, such as when a woman records her ex-husband’s conversations with her as evidence of breach of an intervention order.59 Police also use participant monitoring when gathering evidence for criminal prosecutions.60

6.60 In those Australian jurisdictions where participant monitoring is unlawful (NSW, Western Australia, ACT, South Australia and Tasmania), the legislation contains a range of exceptions. A common exception is where all parties to the conversation or activity consent.61 Other exceptions are outlined directly below.

When reasonably necessary for the protection of lawful interests

6.61 NSW, Tasmania, ACT, Western Australia and South Australia allow participant monitoring by a principal party to the conversation or activity if it is reasonably necessary for the protection of that party’s lawful interests.52 A principal party is one who speaks or is spoken to in the course of the conversation, or who takes part in the activity.63

6.62 The NSW Court of Criminal Appeal has interpreted ‘reasonably necessary for the protection of the lawful interests’ of a principal party narrowly in order to prevent the exception from swallowing the rule.64

50 Ibid.
51 Guardianship and Administration Act 1986 (Vic) s 37.
52 Section 6 of the SDA prohibits a person using a listening device to monitor a private conversation to which the person is not a party. Section 7 contains a similar prohibition on the use of an optical surveillance device.
53 Surveillance Devices Act 2001 (Vic) s 11(1).
54 Note that a person’s conversation might also be secretly recorded by an individual acting for the police. Specifically, the SDA allows a law enforcement officer, without a warrant, to use a listening device to monitor or record a private conversation to which he or she is not a party if at least one party to the conversation consents, and where the officer is acting in the course of his or her duty and believes the recording is needed to protect the safety of any person: Surveillance Devices Act 2001 (Vic) s 6(2)(c).
55 This is what was found to have occurred in Giller v Procopets (2008) 40 Fam LR 378, [2008] VSCA 236.
57 Surveillance Devices Act 1999 (Vic) s 6(1); Invasion of Privacy Act 1971 (Qld) s 43(1)(a); Surveillance Devices Act 2007 (NT) s 11(1).
59 Submission 11.
60 Submission 11.
61 Surveillance Devices Act 2007 (NSW) s 7(3)(a); Surveillance Devices Act 1998 (WA) s 5(3)(c); 6(3)(a); Listening Devices Act 1992 (ACT) s 4(3)(a); Listening Devices Act 1991 (Tas) s 5(3)(a).
62 Surveillance Devices Act 2007 (NSW) s 7(3)(b); Listening Devices Act 1991 (Tas) s 5(3)(b)(i); Listening Devices Act 1992 (ACT) s 4(3)(b)(i); Surveillance Devices Act 1998 (WA) ss 5(3)(c), 6(3) (iii); Listening and Surveillance Devices Act 1972 (SA) s 7(1)(b).
63 See eg, Surveillance Devices Act 1998 (WA) s 3 (‘principal party’).
Modernising the Surveillance Devices Act

6.63 Although ‘reasonably necessary’ means only ‘reasonably appropriate’ (rather than essential),65 the Court held that it was not reasonably appropriate for a sexual assault victim to secretly record the perpetrator admitting to the assault. This was because the victim could have approached the police with his complaints.66

6.64 Thus, the exception does not allow for ‘covert recordings of a conversation by any person who alleges that he or she is a victim of crime, and who speaks to the alleged offender for the purpose of obtaining admissions of offences’.67

6.65 Moreover, what is reasonably necessary is an objective test, having regard to the circumstances that existed at the time the recording was made.68 Thus, it is not sufficient that the surveillance user believed it to be reasonably necessary to protect a lawful interest. The Court also declined to give the term ‘lawful interests’ a broad meaning.69 It held that ‘lawful interests’ do not include an interest in vindicating one’s right not to be a victim of crime.70

Police duties

6.66 NSW, Tasmanian, Western Australian and South Australian surveillance device legislation also exempts participant monitoring by law enforcement officers from the general prohibition against participant monitoring. In the Western Australian legislation, the prohibition against recording a private conversation or a private activity to which a person is a party does not apply to a police officer acting in the course of his or her duty.72 Moreover, the Act also exempts a person who acts under instruction from a law enforcement officer in the course of investigating a criminal offence.73 There is a similar provision in the South Australian legislation.74

6.67 NSW and Tasmania75 have broader exemptions. For example, the NSW legislation exempts a law enforcement officer who is a party to a private conversation and is participating in an authorised operation (within the meaning of the Law Enforcement (Controlled Operations) Act 1997 (NSW)) under an assumed name from the prohibition on the installation, use and maintenance of a listening device.76

Other allowed instances of participant monitoring

6.68 A number of states (NSW, ACT and Tasmania) also allow for participant monitoring by a principal party when the purpose of the recording is not to share it with individuals who are not a party to the conversation or activity.77

6.69 The Tasmanian legislation contains a general exception to the ban on the use of a listening device without consent, where the use is to gain evidence or information in connection with an imminent threat of serious violence, substantial damage to property or serious narcotics offence.78 In such a case, the user must report to the Chief Magistrate within three days after using the device.79 The South Australian legislation allows for participant monitoring if it is ‘in the public interest’.80

Submissions

6.70 There was support in submissions for the proposal in our Consultation Paper that Victoria should prohibit participant monitoring using surveillance devices.81 Liberty Victoria, for example, noted that the reform would promote privacy and consistency between jurisdictions, bringing provisions of the SDA in line with NSW, South Australia, Tasmania, Western Australia and ACT.82
6.71 Those who opposed any change noted the beneficial uses of participant monitoring. For example, Victoria Police argued that the use of participant monitoring enables police to perform important functions such as evidence gathering and the protection of undercover operatives.\(^83\) The Lilydale Centre Safe Committee noted its use by parties in domestic violence and family law matters, such as a woman recording her ex-husband’s conversations with her as evidence of him breaching his intervention order.\(^84\) In fact, the Committee favours such monitoring by both parties, because when they do they ‘tend to be civil to one another averting further breaches and allegations of breaches’.\(^85\)

6.72 One submission suggested that the ban on participant monitoring was ultimately uncontroversial given the prohibition on communicating or publishing the information gained. In consultation with media representatives the commission was told that extending the participant monitoring ban would have little effect on journalistic practices. As one television news executive told the commission, whether participant monitoring should be banned is an academic point because, as it stands, the material obtained through participant monitoring cannot be used.\(^86\)

6.73 In general, submissions in favour of the ban also supported exemptions that would allow participant monitoring in limited circumstances. For example, the St Kilda Legal Service said there should be an exception to allow for evidence gathering in family violence and family law matters:

> Without [such an exemption] individuals may find it more difficult to gather evidence to support their case. This is because in family violence matters, for example, there are often no witnesses to the alleged abuse apart from the victim and the perpetrator.\(^87\)

6.74 Liberty Victoria supported the exceptions now found in the SDA (NSW) ‘which ensure the practice remains legal in limited and appropriate circumstances’.\(^88\) The Office of the Victorian Privacy Commissioner went further, suggesting it would be preferable if the exceptions were warrant-based.\(^89\)

6.75 The commission is of the view that, as a rule, a person should be able to conduct private conversations and engage in private activities without those events being recorded without their consent. Such an expectation is consistent with the overall purpose of surveillance devices legislation, which is to protect privacy by prohibiting the covert use of surveillance devices other than in exceptional circumstances associated with law enforcement. We recommend that the general participant monitoring exception in sections 6(1) and 7(1) of the SDA be removed.

6.76 We accept, however, that in some circumstances this general rule should not apply. Any exceptions to a general prohibition against participant monitoring should not greatly diminish the usual expectation that conversations and activities should not be covertly recorded by anyone.

6.77 There is no need to prohibit participant monitoring when all parties to the conversation or activity consent. The prohibitions in the SDA already provide an exception when each party to a conversation or activity gives their consent, express or implied, to the use of a surveillance device.\(^90\) Consequently, even if the words ‘to which the person is not a party’ are removed from sections 6(1) and 7(1), there is no need to create an additional exception for those instances when each party has given his or her consent to the recording.

Meaning that surveillance was the only means by which a person could protect the lawful interest: Sepulveda v R [2006] NSWSC 379 [139].

Submission 29.

Submission 5.

Submission 14.

Consultation 12.

Submission 11.

Submissions 2, 5, 14, 29, 33.

Submission 5.

Submission 4.

Submission 11.

Submission 4.

Submission 29.

Submission 14.

Submission 5.

Submission 29.

Submission 14.

Submission 5.

Submission 29.

Submission 14.

Submission 5.

Submission 29.

Submission 14.

Submission 5.

Submission 29.

Submission 14.

Submission 5.

Submission 29.

Submission 14.
Chapter 6

Modernising the Surveillance Devices Act

6.78 Participant monitoring by a principal party to a conversation should be possible where it is reasonably necessary for the protection of that party’s lawful interests. This exception should not be too broad. For example, we do not favour the exception recently suggested by the New Zealand Law Commission, which would permit non-consensual recording of a conversation to keep a more accurate record than memory could provide.91

6.79 Although we favour a narrow view of the ‘lawful interests’ exception, we suggest that it should not be as narrow as the one suggested by the NSW Court of Criminal Appeal. We favour an interpretation that allows for participant monitoring for evidentiary purposes, as suggested in a number of the submissions we discussed above.

6.80 Similarly, although we support allowing participant monitoring by law enforcement officers in the course of their duties and without a warrant, we favour limiting the exception to situations in which an officer reasonably suspects the person being recorded has committed an offence or is doing so.

6.81 We have not proposed the exception found in legislation elsewhere that permits a person to engage in covert participant monitoring when the recording is made without the purpose of sharing the material with others. In these circumstances it is still possible that recordings made by a party to a conversation or activity may fall into the hands of third parties. We have also chosen not to recommend a broad public interest exception because its scope is too uncertain for use in a regime that contains criminal sanctions.

RECOMMENDATION

18. Sections 6 and 7 of the SDA should be amended to prohibit participant monitoring using a listening or optical surveillance device subject to the following additional exceptions:

   a. the use of a listening or optical surveillance device by a law enforcement officer to record a private conversation or private activity to which he or she is a party if:

      i) the law enforcement officer is acting in the course of his or her duty; and

      ii) the law enforcement officer reasonably believes at least one party to the conversation or activity of having committed or being in the course of committing an offence

   b. the use of a listening device or optical surveillance device by a party to a private conversation or private activity if:

      i) a principal party to the conversation or activity consents to the listening device being so used; and

      ii) recording of the conversation or activity is reasonably necessary for the protection of the lawful interests of that principal party.
A CIVIL PENALTY REGIME

6.82 The SDA provides criminal sanctions when a person uses a surveillance device, or publishes information gained by the use of a surveillance device, in prohibited ways.92 The more serious offences attract a maximum penalty of two years imprisonment, or a fine of up to 240 penalty units for an individual (1200 penalty units for a corporation), or both.93

6.83 The commission has only been able to find evidence of four successful prosecutions for breach of the SDA since its inception on 1 January 2000. All cases concerned the unlawful use of optical surveillance devices in particularly offensive circumstances.94 One explanation for the small number of prosecutions may be that the criminal sanctions in the SDA are too severe for use in cases where the wrongful behaviour is not highly offensive.

6.84 There is growing support for the use of civil penalties when dealing with many violations of the law. One legislator noted ‘a modern complex society with limited judicial resources and an economic need for efficiency must necessarily seek mechanisms for the enforcement of its rules additional to traditional criminal processes’.95 In 2007 the Commonwealth Attorney-General’s Department stated that civil penalties are most likely to be appropriate and effective where

- criminal punishment is not merited (for example, offences involving harm to a person or a serious danger to public safety should always result in a criminal punishment)
- the penalty is sufficient to justify court proceedings
- there is corporate wrongdoing.96

6.85 These matters were considered by the ALRC when it recommended a civil penalties regime for breaches of the Privacy Act 1988 (Cth).97 The ALRC concluded that ‘criminal sanctions would be disproportionate to the level of harm caused by a serious or repeated interference with an individual’s privacy’.98

6.86 In our Consultation Paper we suggested the introduction of a civil penalty regime for existing offences in the SDA. This would allow a surveillance regulator to act on the less serious matters that come to his or her attention without referring the matter to Victoria Police.

6.87 Introducing civil penalties is also likely to reduce the cost and complexity of the regulatory process.99 This is consistent with the current approach taken by the Victorian government, which ‘continues to work towards minimising [the regulatory] burden’ on ‘businesses, not-for-profit organisations, government sector organisations … and society as a whole’.100

6.88 A number of federal oversight bodies have the power to bring civil penalty proceedings, including the Australian Competition and Consumer Commission (ACCC),101 Australian Securities and Investment Commission (ASIC),102 and the Environment Protection Authority (EPA).103 Civil penalty orders are available under many pieces of Commonwealth legislation.104

6.89 In Victoria, there has also been growing use of civil penalties. For example, the Essential Services Commission is responsible for bringing civil penalty proceedings under a number of Acts, including the Essential Services Commission Act 2001 (Vic),105 the Rail Corporations Act 1996 (Vic),106 and the Victorian Renewable Energy Act 2006 (Vic).107 The courts may make a civil penalty order under the Outworkers (Improved Protection) Act 2003 (Vic)108 and the Long Service Leave Act 1992 (Vic).109 VCAT may make a civil penalty order under the Owners Corporation Act 2006 (Vic).110
Modernising the Surveillance Devices Act

6.90 There was broad support for the introduction of a civil penalty regime among submissions to the commission. The Victorian Privacy Commissioner argued that one reason the current criminal regime was ineffective was due to an inherent conflict of interest: the police who prosecute illegal uses of surveillance devices also have an interest in obtaining footage from third parties to assist their investigations.111

6.91 The Federation of Community Legal Centres supported civil penalties but also promoted an educational approach.112 Victoria Police noted they seek ‘protection from liability for police officers acting for a lawful purpose in the course of their duties’.113

6.92 The commission believes that a greater range of regulatory measures should be available to control the use of surveillance in Victoria.

6.93 In our Consultation Paper we noted it may be appropriate to retain criminal penalties in the SDA if a civil penalties regime is introduced. The introduction of civil penalties should not restrict police from pursuing criminal prosecutions under the existing provisions of the SDA, or for surveillance-related offences in other Acts. This includes those dealing with stalking,114 indecent, offensive or insulting behaviour115 and ‘upskirting’.116 A number of federal regulators, including the ACCC117, ASIC118 and the EPA, have the power to bring civil penalty proceedings when criminal prosecutions are also available.119

**RECOMMENDATION**

19. Sections 6–9 and 11–12 of the SDA should be amended to include civil penalties as an alternative to criminal penalties. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.

**A NEW OFFENCE FOR IMPROPER USE OF A SURVEILLANCE DEVICE**

6.94 The SDA currently regulates the use of four types of devices: listening devices, optical surveillance devices, tracking devices and data surveillance devices.120 The commission has recommended changes to modernise these provisions and to fill gaps that have become apparent over time. In addition, we have considered whether the SDA should be amended to include a new offence that would prohibit offensive surveillance practices regardless of the type of device actually used. The primary purpose of such a new offence would be to send a clear message to the community that various forms of behaviour with a surveillance device are unacceptable.

6.95 A number of submissions noted the desirability of ensuring the SDA is sufficiently flexible to cover new and emerging uses of surveillance.121 Although the commission agrees with these views, it is difficult to prohibit particular uses of unknown devices with the precision necessary for a criminal offence. The commission has concluded, however, that there is merit in introducing a new offence which prohibits unacceptable behaviour with a surveillance device.
6.96 The commission is aware of a number of instances of surveillance devices being used to intimidate, demean or harass people. For example, in submissions and consultations we learnt about individuals filming violence for entertainment—a practice known colloquially as ‘happy slapping’. For example, in 2007 a group of young people lured a teenage girl to a park and sexually assaulted her, set fire to her hair and urinated on her. They filmed the incident and distributed the footage on DVD. Other examples include an incident at a secondary school in Pakenham, where a fight between students was recorded on another student’s mobile phone. Other school yard assaults have also been captured on mobile phone cameras, with those behind the camera audibly encouraging the violence. In some cases the use of a surveillance device may exacerbate criminal behaviour. For example, in one case, it was reported that a man waved at a camera during a sexual assault.

6.97 The fact that the images can be distributed widely and quickly further compounds the problem. One academic stated that ‘the internet actually encourages this behaviour because kids from all over the world go on and rate the fights, so … this particular medium may be encouraging violence’. Surveillance devices can be used to record highly personal information. In a recent case, Giller v Procopets, the defendant covertly filmed the couple’s consensual sexual activity and later threatened to show the plaintiff’s family and friends the videotapes. This sort of behaviour should be strongly discouraged. In Chapter 4 we also noted media reports of an increase in individuals using devices such as camera phones to capture images of other people in distress during emergencies. Recent examples include incidents in which people have filmed the aftermath of traffic accidents. In one instance, onlookers filmed the dying moments of a man after a car hit him. Filming an emergency in order to assist emergency services is quite different to filming an emergency for entertainment purposes.

111 Submission 29.
112 Submission 40.
113 Submission 11.
114 Crimes Act 1958 (Vic) s 21A.
115 Summary Offences Act 1966 (Vic) s 17.
116 Summary Offences Act 1966 (Vic) ss 41A, 41B, 41C.
118 Under the Corporations Act 2001 (Cth).
119 Under the Environmental Protection and Biodiversity Conservation Act 1999 (Cth).
120 Surveillance Devices Act 1999 (Vic) ss 6–9.
121 Submissions 11, 29, 33, 36.
123 See Cooper, above n 122.
130 Michael, above n 129.
Modernising the Surveillance Devices Act

6.100 Sometimes surveillance devices are used for the purpose of intimidation or to prevent people from doing something they are otherwise lawfully entitled to do. Some submissions to our Consultation Paper expressed concern about surveillance being used in this manner. Local examples include anti-abortion campaigners setting up surveillance outside abortion clinics and people being filmed entering gay bars or drug treatment clinics.

6.101 In consultations and submissions concern was expressed at the power relationship that exists between users of surveillance and people under surveillance. At the extreme end of the scale, classic cases of blackmail involve the threat of the release of personal or embarrassing information. Submissions gave examples of people involved in an embarrassing incident who have been recorded, and then the footage later broadcast on television or uploaded to the internet.

OTHER JURISDICTIONS

6.102 Some other countries have criminalised the act of filming violence for entertainment. For example, in 2007, the French government inserted provisions into its criminal code as a response to the rising incidences of ‘happy slapping’. Now, only professional journalists may film real-world violence and distribute it on the internet. The offence is punishable by up to five years imprisonment and/or a fine of up to €75,000.

6.103 The New Zealand Law Commission has recently delivered its final report into invasion of privacy. Recommendations include strengthening and streamlining prohibitions against inappropriate uses of surveillance devices. For example, the Commission recommends that the sections of the Crimes Act 1961 (NZ) dealing with intimate visual recordings (which aim to prevent the filming of a person’s sexual activity or intimate areas without their consent) should be moved into their proposed new Surveillance Devices Act. Further, the Commission recommends that ‘keeping a person under surveillance’ should be added as a specified form of surveillance regulated under the Harassment Act 1997 (NZ).

6.104 Newspaper articles from the UK cite particularly violent incidents of happy slapping, including instances in which a victim ultimately died from their injuries. In the UK there is no specific offence prohibiting filming violent attacks for entertainment, however, other offences may be used to deal with this behaviour. In 2008 a teenager who used her mobile phone to film the fatal bashing of a man pleaded guilty to aiding and abetting manslaughter, even though she did not physically participate in the attack. She was sentenced to two years imprisonment.

6.105 The commission is of the view that it is desirable to introduce a new offence that demonstrates clear community disapproval of the growing use of a surveillance device to intimidate, demean or harass people. There is considerable educative value in a strong legislative statement that it is unacceptable to use a surveillance device for these purposes. Although there are already some offences concerning certain specific uses of surveillance devices, such as stalking or ‘upskirting’, and while offensive behaviour of any nature in a public place is unlawful, there is no specific offence concerned with the grossly offensive use of a surveillance device.
6.106 The SDA currently prohibits the publication or recording of a private conversation or private activity. The current SDA prohibitions are limited to private conduct. These provisions do not apply where parties ought reasonably to expect that someone else could observe what they are doing or saying. Many of the inappropriate uses of surveillance devices would probably constitute an offence of obscene, indecent or offensive behaviour under the Summary Offences Act 1966 (Vic). This longstanding offence does not provide the community with a clear message, however, that use of a surveillance device to intimidate, demean or harass another person is unacceptable. The commission is of the view that a separate offence in the SDA would appropriately serve this purpose.

6.107 The new offence should apply in two situations. First, where a surveillance device is used to intimidate, demean or harass a person of ordinary sensibilities. Secondly, where a surveillance device is used to prevent or hinder a person from performing an act they are lawfully entitled to do. This latter situation includes, for example, using a surveillance device to discourage people from entering places such as abortion clinics or gay bars.

6.108 Some submissions expressed concern that any amendments to the SDA should avoid criminalising legitimate uses of surveillance devices. We believe that the proposed new offence strikes an appropriate balance and would not outlaw acceptable uses of surveillance devices. For example, the use of a surveillance device by the media to record the aftermath of a natural disaster is part of their legitimate newsgathering activity, and is not conducted for the purpose of intimidating, demeaning or harassing an individual.

RECOMMENDATION

20. A new offence should be included in the SDA that makes it unlawful to use a surveillance device in such a way as to:
   a. intimidate, demean or harass a person of ordinary sensibilities; or to
   b. prevent or hinder a person of ordinary sensibilities from performing an act they are lawfully entitled to do.

21. A civil and alternative criminal penalty should apply for breach of the offence. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.

CONCLUSION

6.109 At present the SDA regulates the use of surveillance devices inconsistently—certain activities are prohibited while others are effectively permitted because the Act says nothing about them. Furthermore, breaches of the Act attract serious criminal sanctions, which have proven not particularly effective in regulating public place surveillance. In this chapter we have explained our recommended changes to the Act to address these shortcomings, and to modernise the way in which the use of surveillance devices is regulated.