Guidelines to surveillance and privacy in the Victorian public sector

Issued May 2017

Commissioner for Privacy and Data Protection

VICTORIA State Government

This page is intentionally left blank.

Guidelines to surveillance and privacy in the Victorian public sector

Issued May 2017

Published by the Commissioner for Privacy and Data Protection
PO Box 24014
Melbourne Victoria 3001

First published May 2017

Also published on:
http://www.cpdp.vic.gov.au

ISBN 978-0-6480788-4-5

DOCUMENT DETAILS	
Security Classification	Public domain
Version	V.01
Issue Date	May 2017
Document Status	Final
Authority/Approval	Office of the Commissioner for Privacy and Data Protection (CPDP)

This page is intentionally left blank.

Introduction

There are many technologies that are capable of being used to observe or monitor individuals or groups. Closed-circuit television (CCTV), unmanned aerial vehicles (drones), internet and phone monitoring, biometric surveillance such as facial recognition, and geo-location tracking are some of the commonly used surveillance technologies, the purposes for which vary greatly. Such technologies offer their users the ability to gather information that may not otherwise be generated.

These guidelines have been produced to offer the Victorian public sector a set of best practice principles for using surveillance technologies in a privacy-enhancing way. In many instances the information generated by these devices will be personal information, such as an image of an individual, written information, or a voice recording. Where personal information is collected by a Victorian public sector organisation the *Privacy and Data Protection Act 2014* (PDPA) will apply. In some cases, organisations will also have obligations under other legislation in relation to surveillance.

The principles offered in these guidelines were collated from a number of resources from Australia and around the world on the responsible use of surveillance technologies, and have been adapted to align with the Information Privacy Principles (IPPs) under the PDPA. A full reference list is included at the end of this document for further reading.

The guidelines have been designed to consider best practices for *overt* surveillance activities only. Some organisations, such as Victoria Police and other law enforcement bodies, may have a unique authority to conduct covert surveillance operations, to which most organisations will not be privy. Independent legal advice should be sought before undertaking any covert surveillance activities. The guidelines are also limited to surveillance use in *public* places.[1]

The guiding principles are intentionally technology-neutral, recognising that regardless of the type of surveillance activity, the privacy issues will be comparable. As such the guidelines have been written to reflect the relevant considerations for *all* types of public sector surveillance.

The way that surveillance technologies are designed and deployed will determine the effect they have on individuals' privacy. By thinking about privacy *prior* to implementing a surveillance program, organisations can mitigate risks and minimise the privacy-invasive nature of their activities. These guidelines offer a starting point for organisations wishing to pursue business objectives through surveillance activities, while respecting individuals' right to privacy.

1 The Victorian Law Reform Commission defined a public place as "any place to which the public have access as of right or by invitation, whether express or implied and whether or not a charge is made for admission to the place". See *Surveillance in Public Places: Final Report 18*, 2010, p. 22.

Surveillance use in the public sector

Defining surveillance

The Victorian Law Reform Commission (VLRC) has defined surveillance as "the deliberate or purposive observation or monitoring of a person, object or place".[2] Monitoring and observation activities can be conducted systematically as part of an ongoing program, or may be ad hoc in response to an identified need, such as an emergency.

There are various categories of surveillance, including:

- optical or visual surveillance
- audio surveillance
- tracking or location surveillance
- physical surveillance
- data surveillance
- biometric surveillance.

Surveillance is typically an intentional act done for a specific purpose, rather than an incidental consequence of some other activity.[3] There are a variety of reasons why a public sector organisation may choose to engage in surveillance activities. Common purposes include:

- investigation of crime
- crime prevention and deterrence
- national security
- enhancing personal safety of members of the public and public servants
- search and rescue operations.

Commonly used surveillance technologies

As technologies are becoming cheaper and more accessible, there is no shortage of options available to public sector organisations wishing to initiate surveillance programs. Some of the more common surveillance technologies and methods used by the public sector are outlined below.

Closed-circuit television

CCTV is a type of video surveillance, and is one of the most commonly used surveillance devices. CCTV cameras are generally fixed into position, for example against a wall, and can be pointed in a chosen direction to capture activity in a defined space. CCTV cameras are a popular option in public places due to the perception – whether accurate or not – that their mere presence increases safety and prevents crime.[4]

2 Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18*, 2010, p. 9.

3 Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18*, 2010, p. 21.

4 The Australian Institute of Criminology has undertaken research into the effectiveness that CCTV cameras have on reducing crime. See *Considerations for establishing a public space CCTV network*, Resource manual no. 8, 2009.

There are two types of CCTV use:

- *Pro-active* CCTV: footage is monitored live, for example by the police or a security unit. This footage may or may not be recorded.
- *Re-active* CCTV: involves recording and storing the footage captured by the camera for viewing at a later date, if required.[5] Re-active CCTV is the most common form used, as it is less resource intensive and the footage can be re-watched multiple times.

Unmanned aerial vehicles

Unmanned aerial vehicles (UAVs) – more commonly known as *drones* – are aircrafts that are operated remotely without a person on board to control them.[6] While not strictly a surveillance technology, drones can be equipped with cameras or audio equipment to enable them to be deployed for the purpose of gathering information. Drones can often fly for extended periods of time given that there is no pilot on board. Coupled with their mobility, UAVs are often a desirable surveillance technology.

Some of the common uses for drones within the public sector include search and rescue operations; aiding responses to natural disasters, such as locating and tracking fires; traffic monitoring; and national security intelligence gathering.[7] These surveillance activities may not necessarily be carried out with the intention of collecting personal information, however operators should note the potential for individuals to be identified.

Body worn cameras

Body worn cameras are a type of CCTV often worn on clothing, enabling up-close recording of video footage. Some cameras may also be equipped with an audio recording capability. Body worn cameras are fast becoming a popular option amongst law enforcement agencies and other public servants, such as parking inspectors, who may face a risk to their safety. Law enforcement officers that favour wearing body worn cameras are often of the view that the cameras are effective in reducing violent or aggressive behaviour from members of the public and that they are a useful evidence-gathering tool, although their effectiveness is a subject of debate.[8]

Communications surveillance

Communications surveillance is the monitoring, interception, collection and retention of information that has been relayed over communications networks, such as the internet, mobile phones, or fixed phone lines.[9] Communications surveillance can be conducted on a mass scale or targeted at individuals or groups. A number of governments around the world – including the Australian Government – have introduced mass data retention schemes in response to national security concerns, whereby telecommunications information is collected and used to monitor criminal activity and identify persons of interest.

---

5 Department of Justice, *Guide to developing CCTV for public safety in Victoria: A community crime prevention initiative*, Community Crime Prevention Unit, 2011, p. 23.

6 Office of the Privacy Commissioner of Canada, *Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, 2013, p. 2.

7 U.S. Department of Homeland Security Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft* Programs, U.S. Department of Homeland Security, 2015, p. 3; Office of the Privacy Commissioner of Canada, *Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, 2013, p. 5; House of Representatives Standing Committee on Social Policy and Legal Affairs, 'Drones and privacy', *Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy*, 2014, p. 33.

8 Darren Palmer, 'The mythical properties of police body-worn cameras: A solution in the search of a problem', *Surveillance & Society*, Vol. 14, No. 1, 2016, pp. 138-44.

9 Privacy International, *Communications Surveillance*, accessed at https://www.privacyinternational.org/node/10.

Privacy challenges

Surveillance practices have the potential to impinge upon individuals' privacy if the appropriate steps are not taken to uphold this right. Some of the privacy risks that surveillance may pose include:

- **Function creep:** information collected for one purpose is then used for another purpose at a later time. This risk is exacerbated where information is retained for long periods of time without adequate measures in place to manage how it is handled.
- **Lack of transparency:** individuals are not made aware that they are under surveillance and do not understand what the information will be used for.
- **Intrusiveness:** depending on where surveillance activities take place and what they capture, practices may be considered unreasonably intrusive and disproportionate to the purpose they are trying to achieve.
- **Over-collection:** surveillance activities may generate and capture more information than is necessary – for example, a body worn camera could film individuals in the background when recording an up-close incident.

In addition to information privacy, surveillance can also threaten other forms of privacy, such as locational and territorial privacy. Users of surveillance technologies should take into consideration these broader aspects of privacy when engaging in surveillance activities.

Guiding principles for surveillance use

The following principles provide a starting point from which public sector organisations can begin to consider their obligations with respect to privacy when planning to undertake surveillance activities. Each organisation may also be bound by its own enabling legislation and a series of other laws that have an impact on surveillance use. As such there are broader considerations beyond information privacy that should also inform an organisation's approach to surveillance – these principles are merely one set of factors that should be taken into account.

1. Surveillance use must always be necessary, proportionate and for a legitimate purpose related to the activities of the organisation.

An organisation should only use surveillance where this practice is necessary for one of the organisation's functions or activities.[10] Surveillance should not be used simply because it is the most cost effective and convenient means to achieve an objective – the benefits of surveillance must substantially outweigh any intrusion on privacy.[11] Organisations should be able to clearly define the problem they are trying to solve through the use of surveillance technologies and be able to justify why they are necessary to address that problem.

It is also important when using surveillance technologies that only the minimum amount of personal information necessary is collected and retained. Where possible, surveillance devices should be calibrated to avoid over-collecting personal information, such as blurring background images in visual recordings,[12] or limiting the hours of operation.[13]

Surveillance use must also be proportionate to the problem being addressed.[14] For example, it may not be a proportionate response for a school principal to install CCTV cameras in all classrooms as a result of an isolated complaint from a parent about one teacher. Organisations should consider their purpose for undertaking surveillance activities and ensure that they are only used in the absence of less privacy-invasive alternatives.

2. Individuals are entitled to a reasonable expectation of privacy in public places.

Organisations should refrain from using surveillance in places where individuals may reasonably expect to have a degree of privacy. This may include some public spaces, such as change rooms in community leisure centres, public toilets in a park, and restrooms in a place of employment.[15]

10 IPP 1.1, Schedule 1, *Privacy and Data Protection Act 2014*.

11 Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014, p. 4.

12 Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014, p. 5.

13 New Zealand Privacy Commissioner, *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations*, 2009.

14 Victorian Law Reform Commission, *Surveillance in Public Places*, Final report 18, 2010.

15 Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014, p. 6.

In its final report into *Surveillance in public places*, the Victorian Law Reform Commission identified a number of factors that may inform a 'reasonable' expectation of privacy with regard to surveillance. Some of these include:

- the type of place under observation
- the nature of the activity taking place
- the type of surveillance in use
- the identity of the individual or individuals under observation – for example, a celebrity may have a different expectation of privacy than an everyday citizen making their commute to work.[16]

When deciding where to position surveillance devices, it is important to note that practices which may be permissible under privacy law might not necessarily align with the public's expectation of reasonable privacy. For example, IPP 2.1 permits an organisation to disclose an individual's personal information for a number of secondary purposes. Although it may be authorised under legislation, an individual might not expect their image or communications data to be shared with third parties without their consent. Expectations of privacy should be balanced against necessity in such circumstances – just because an act or practice is legal, it doesn't necessarily mean it should be done.

Taking the public's expectations into account, organisations should carefully consider where they would position surveillance devices before they begin to use them. This is particularly relevant for mobile devices, such as body worn cameras and drones. Policies should be put in place to ensure that the operators of these devices are aware of where they can and cannot be used.

3. Surveillance operators must assess the impact of the proposed surveillance before it is undertaken.

Before an organisation decides to commence a surveillance program, there are a number of steps that should be taken to assess whether or not the surveillance is appropriate, and to identify and mitigate any risks that could arise.

Organisations should always consider consultation with the community in the first instance.[17] This will assist them to determine whether or not surveillance is an appropriate option to address the identified problem and whether the public are comfortable with a surveillance program in their community. Speaking with other stakeholders and organisations that have implemented surveillance programs is also a useful way to help identify risks and learn from others' experiences.[18]

Any public sector program that involves personal information should always be subject to a privacy impact assessment (PIA), security risk assessment, and a human rights impact assessment. These steps will enable organisations to identify any privacy and security risks upfront and implement measures to mitigate against them before the program commences, and ensure that the program does not breach the *Charter of Human Rights and Responsibilities Act 2006*. The CPDP website contains information on how to complete a PIA (including a template) and security risk assessment.

It is also important for organisations to consider the need to engage with Victoria Police regarding their surveillance activities, as there may be safety issues involved and implications if criminal activity is identified.

16 Victorian Law Reform Commission, *Surveillance in Public Places*, Final report 18, 2010, p. 86.
17 Office of the Information Commissioner Queensland, *Camera surveillance and privacy*, 2015, p. 3.
18 Victorian Ombudsman, *Closed circuit television in public places – Guidelines*, 2012, p. 5.

4. Surveillance use must be consistent with applicable laws and standards.

An organisation's enabling legislation will be the primary piece of legislation that sets out its functions and how it is required, or permitted, to handle information in respect of those functions. Organisations must ensure that they have the legal authority under their own legislation to collect, use and disclose personal information for the purpose of a surveillance program. The PDPA is default legislation, which means that where an organisation's enabling legislation is silent on information handling, they will be required to comply with the provisions of the PDPA in that regard.

In addition to the PDPA, there are a number of other pieces of Victorian legislation that may be applicable to organisations undertaking surveillance activities. These include, but are not limited to:

- *Surveillance Devices Act 1999*
- *Public Records Act 1973*
- *Freedom of Information Act 1982*
- *Charter of Human Rights and Responsibilities Act 2006*.

Standards Australia has also released a voluntary standard on CCTV, which provides recommendations on the operation and management of CCTV, including privacy considerations.[19] While not mandatory, organisations should be aware of this and other best practice guidance on CCTV and surveillance devices in general when planning their own surveillance programs.

5. Surveillance activities should be governed by policies, operating procedures and agreements.

Prior to commencing surveillance activities organisations should develop clear internal policies and procedures for the operation of the program. Having these in place will ensure that all staff involved in the program are aware of their individual obligations and understand how the information captured by surveillance activities should be handled. These documents should be communicated to relevant employees and be easily accessible at all times.

Policies and procedures for surveillance should include the following at a minimum:

- the purpose of the surveillance program
- what information is collected and how it is used and stored
- who is permitted to access the information
- the roles that are responsible for the management of surveillance activities
- the protocols to be followed for ensuring the security of information
- for how long the information will be retained
- relevant legislation that governs the surveillance program
- who the appropriate contact is within the organisation, should staff or members of the public have questions about the program
- processes for receiving complaints and managing privacy breaches.

19 Standards Australia, *Closed circuit television (CCTV): Part 1 Application and Management*, AS 4806.1, 2006.

Where there is more than one party involved in managing the surveillance program, appropriate agreements should be in place to set out responsibilities, accountabilities and expectations.[20] For example, where a local council is relying on Victoria Police to either monitor or review CCTV footage, the conditions under which this will be done should be set out in a memorandum of understanding (MOU). Further, if an organisation engages a contracted service provider (CSP) to manage all or part of the surveillance program, it must ensure that a contract sets out the agreed upon governance arrangements and responsibilities for each party involved, including which party retains liability for privacy obligations under the PDPA. This also applies to cloud services that are used to facilitate the storage or processing of information.[21]

6. Surveillance operators should undergo privacy training prior to use.

All employees who operate surveillance equipment, handle the information captured, or oversee a surveillance program should undergo privacy training.[22] Providing training to staff is critical for ensuring that they are aware of their information handling obligations under the PDPA and internal organisational policies, and promotes a consistent approach to protecting personal information. Training also empowers staff to confidently make decisions about how to use, store, disclose and dispose of the information captured, minimising the potential for privacy breaches.

7. Surveillance operators must take reasonable steps to inform individuals of the use of surveillance devices.

Whenever a public sector organisation collects personal information about an individual, it must take steps to notify the individual accordingly. Providing notice of collection improves transparency and trust between an organisation and the public. Individuals should be made aware of matters such as:

- which organisation is collecting the information
- the purpose for which the information is collected
- to whom the information may be disclosed
- that the individual has a right to access the information held about them.[23]

Making individuals aware of the identity of the organisation collecting their information is critical, as individuals have a right to make enquiries or submit a complaint to the organisation if they feel their privacy has been breached.

When surveillance devices are used in public places, the operator should ensure that appropriate signage is placed around the area under surveillance to inform individuals that they may be under observation.[24] Where possible, notice should ideally be provided *before* an individual enters the site of surveillance, so they can choose whether or not to enter that area.[25]

---

20 UK Home Office, *Surveillance camera code of practice*, 2013, p. 15.

21 CPDP has produced guidelines on outsourcing in the Victorian public sector, available at www.cpdp.vic.gov.au.

22 As a starting point, CPDP offers free privacy training via an online module, available at www.cpdp.vic.gov.au. Further tailored training for surveillance may need to be provided by organisations.

23 IPP 1.3, Schedule 1, *Privacy and Data Protection Act 2014*.

24 Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014, p. 6.

25 Office of the Information Commissioner Queensland, *Camera surveillance and privacy*, 2015, p. 3.

Informing the public that they may be under surveillance when a mobile device is in use may not be as simple as putting up signage, as there will not necessarily be a defined area under observation. When using mobile surveillance devices such as drones, operators may consider alternative forms of notice – for example, running a public advertisement or prominently displaying notice on the organisation's website. While IPP 1.3 prescribes the content of notice, there is no mandated form that a collection notice must take.

Organisations can also take a layered approach to providing notice. This means that the initial notice that the public first sees – in the form of a sign, for example – may contain only a small amount of information, enough to inform individuals that a surveillance device is in operation and which organisation is conducting the activity. It may be reasonable to then provide further information on that activity in another place, such as on the organisation's website, provided that individuals are aware that further information is available should they wish to see it. Ultimately, an organisation's privacy policy should reference their use of surveillance and contain detailed information about their information handling practices.

8. The right of individuals to access their personal information should be respected.

A fundamental principle of privacy law is that individuals have a right to seek access to the personal information an organisation holds about them. In some circumstances it may not be appropriate for the organisation to disclose the information to an individual – for example, where doing so would infringe upon the privacy rights of another person, or the information relates to legal proceedings between the individual and the organisation.[26] However, a surveillance operator should seek to accommodate an individual's access request to the extent possible. Removing or redacting another individual's personal information from the data could be one way to uphold access rights while maintaining the obligation to protect personal information.

The *Freedom of Information Act 1982* is the primary piece of Victorian legislation that covers individuals' right of access to information held about them by public sector organisations.[27] The Freedom of Information Commissioner can provide guidance to organisations regarding the process of determining whether or not it is appropriate to provide individuals with access to the information they are seeking.[28]

9. Reasonable steps should be taken to secure equipment and protect information gathered through surveillance activities.

Data security is a critical component of any surveillance program. Public sector organisations have an obligation to protect the personal information they hold from being misused, lost, or accessed, modified or disclosed by unauthorised persons.[29] The PDPA does not stipulate *how* this is to be done, only that organisations must take 'reasonable steps'.

26 IPP 6.1, Schedule 1, *Privacy and Data Protection Act 2014*.

27 IPP 6 – Access and Correction – was designed to fill a gap in the *Freedom of Information Act 1982* to extend access and correction rights to individuals whose personal information is held by contracted service providers.

28 Visit www.foicommissioner.vic.gov.au for further information.

29 IPP 4.1, Schedule 1, *Privacy and Data Protection Act 2014*.

The safeguards that are put in place should reflect the value of the information captured by surveillance devices. Organisations should keep in mind CPDP's five-step action plan when it comes to the implementation of 'reasonable security':

1. Identify your information assets.
2. Determine the value of this information.
3. Identify any risks to this information.
4. Apply security measures to protect the information.
5. Manage risks across the information lifecycle.

CPDP has produced a guidance document outlining the measures that can be taken to protect information, which includes a discussion on how to determine which steps may be 'reasonable' in a given situation. These measures are drawn from the Victorian Protective Data Security Framework and accompanying standards, developed by the Commissioner under Part 4 of the PDPA. The guidelines are available on the CPDP website.[30]

Security measures should address governance and the core security domains of information security, personnel security, ICT security and physical security. Examples include:

- **Governance:** having the right policies, processes and procedures in place.
- **Information security:** information is protectively marked to indicate handling requirements.
- **Personnel security:** personnel tasked with managing the information are eligible and suitable for the role.
- **ICT security:** ICT controls are implemented to protect the confidentiality, integrity and availability of the information.
- **Physical security:** information is physically stored in a way that minimises any risk to access or tampering.

10. Disclosure of information gathered through surveillance activities should only occur where necessary for the stated purpose, or for a law enforcement purpose.

One of the central principles of privacy law is that personal information collected for one purpose should not then be used or disclosed for another purpose. Generally, organisations should only disclose information in a way that is consistent with the notice provided to individuals – if an organisation can foresee a purpose for which it will need to disclose an individual's personal information, it should communicate this to the individual at the time of collection.

For example, a council that has installed CCTV cameras along a shopping strip to detect crime may have a relationship with a local police station that monitors or accesses the footage as need be. This disclosure relates to the purpose for which video footage is collected, and as such, the fact that the council shares information with Victoria Police should be included in the council's collection notice and privacy policy.

However, there may be exceptional circumstances under which it is appropriate to disclose personal information, provided it is authorised by law. One example is for a law enforcement purpose. IPP 2.1 permits an organisation to disclose personal information where it suspects unlawful activity, or where it is necessary for a law enforcement function, such as the investigation of crime or in relation to court proceedings.[31]

---

30 *Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1*, available at www.cpdp.vic.gov.au.

31 IPP 2.1(e) and (g), Schedule 1, *Privacy and Data Protection Act 2014*.

Information sharing arrangements, whether ongoing or ad hoc, should be appropriately governed by agreements or MOUs. See CPDP's guidelines on information sharing for further guidance on disclosure.[32]

11. Information gathered through surveillance activities should be deleted once it is no longer required.

When planning a surveillance program, an organisation should consider what processes it will put in place to destroy personal information once it is no longer required,[33] including how it will be destroyed and whether de-identification is viable. The Public Record Office of Victoria (PROV) sets retention and disposal authorities that public sector organisations are required to comply with – in some cases information may need to be retained for a period of time despite an organisation no longer having a use for it. If necessary, advice should be sought from PROV regarding retention and disposal obligations.

Retaining personal information captured by surveillance devices for any longer than is necessary can increase an organisation's risk of a privacy breach occurring if that information in misused or accessed by unauthorised personnel. With increasingly sophisticated technologies the potential for facial recognition capability with video surveillance and subsequent data matching is a further privacy risk to individuals if information is retained indefinitely.[34]

12. Effective review and audit mechanisms should be in place to ensure legal requirements and policies are complied with, and that the program is meeting its intended objectives.

An organisation should have in place mechanisms to review and evaluate their surveillance program, to ensure that it is meeting the objectives it set out to achieve and is effective in doing so.[35] Evaluations should be conducted on a regular basis, and changes made to the program as required. If the objectives of using surveillance are not being met the organisation should reconsider its use, as personal information should only be collected if it is *necessary*. Evaluations can be undertaken internally, but obtaining the services of an independent auditor is also an advisable option.[36]

As an organisation's regulatory or operational environment shifts, it should consider whether its obligations regarding information handling and privacy change, and what this means for its surveillance activities. Internal policies and procedures may need to be updated in this respect, and governance arrangements may alter.

An important part of reviewing and evaluating a surveillance program is seeking the views of the community. Consultation with the public should be a valued step in planning for a surveillance program, but it is equally important to engage those affected by the activities during the review process. Privacy is not a static concept, and individuals' preferences and expectations may change through their lived experiences.

---

32 *Guidelines for sharing personal information*, available at www.cpdp.vic.gov.au.

33 IPP 4.2, Schedule 1, *Privacy and Data Protection Act 2014*.

34 Office of the Privacy Commissioner of Canada, *Guidelines for the use of video surveillance of public places by police and law enforcement authorities*, 2006.

35 Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014, p. 9.

36 Office of the Privacy Commissioner of Canada, *Guidelines for the use of video surveillance of public places by police and law enforcement authorities*, 2006.

Reference list

Australian Institute of Criminology, *Considerations for establishing a public space CCTV network*, Resource manual no. 8, 2009.

Darren Palmer, 'The mythical properties of police body-worn cameras: A solution in the search of a problem', *Surveillance & Society*, Vol. 14, No. 1, 2016.

Department of Justice, *Guide to developing CCTV for public safety in Victoria: A community crime prevention initiative*, Community Crime Prevention Unit, 2011.

House of Representatives Standing Committee on Social Policy and Legal Affairs, 'Drones and privacy', *Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy*, 2014.

New Zealand Privacy Commissioner, *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations*, 2009.

Office of the Privacy Commissioner of Canada, *Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, 2013.

Office of the Commissioner for Privacy and Data Protection, *Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1*, 2016.

Office of the Information Commissioner Queensland, *Camera surveillance and privacy*, 2015.

Office of the Information & Privacy Commissioner for British Columbia, *Public sector surveillance guidelines*, 2014.

Office of the Privacy Commissioner of Canada, *Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, 2013.

Privacy International, *Communications Surveillance*, accessed at https://www.privacyinternational.org/node/10.

Standards Australia, *Closed circuit television (CCTV): Part 1 Application and Management*, AS 4806.1, 2006.

UK Home Office, *Surveillance camera code of practice*, 2013.

U.S. Department of Homeland Security Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft* Programs, U.S. Department of Homeland Security, 2015.

Victoria Police, *Community crime prevention program – CCTV information*, accessed at http://www.police.vic.gov.au/content.asp?Document_ID=32487, 2017.

Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18*, 2010.

Victorian Ombudsman, *Closed circuit television in public places – Guidelines*, 2012.

This page is intentionally left blank.

Commissioner for Privacy and Data Protection

VICTORIA State Government