Queensland
Law Reform Commission

Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies

Consultation Paper

WP No 77
December 2018

Queensland
Law Reform Commission

Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies

Consultation Paper

WP No 77
December 2018

Postal address: PO Box 13312, George Street Post Shop, Brisbane, Qld 4003
Telephone: (07) 3247 4544
Facsimile: (07) 3247 9045
Email: lawreform.commission@justice.qld.gov.au
Website: www.qlrc.qld.gov.au

ISBN: 978-0-6481164-2-4

SUBMISSIONS

You are invited to make a written submission on the issues raised in this Consultation Paper. Submissions should be sent to:

The Secretary

Queensland Law Reform Commission
PO Box 13312
George Street Post Shop, Brisbane, Qld 4003

Email: lawreform.commission@justice.qld.gov.au
Facsimile: (07) 3247 9045

Closing date: 31 January 2019

PRIVACY AND CONFIDENTIALITY

Any personal information you provide in a submission will be collected by the Queensland Law Reform Commission for the purposes of its review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies.

Unless you clearly indicate otherwise, the Commission may refer to or quote from your submission and refer to your name in future publications for this review. Further, future publications for this review will be published on the Commission's website.

Please indicate clearly if you do not want your submission, or any part of it, or your name to be referred to in a future publication for the review. Please note however that all submissions may be subject to disclosure under the *Right to Information Act 2009* (Qld), and access applications for submissions, including those for which confidentiality has been requested, will be determined in accordance with that Act.

COMMISSION MEMBERS

Chairperson:	**The Hon Justice David Jackson**
Part-time members:	**The Hon Margaret Wilson QC** **Ms Penelope White** **Dr Nigel Stobbs** **Ms Ruth O'Gorman**

SECRETARIAT

Director:	**Mr David Groth**
Assistant Director:	**Mrs Cathy Green**
Secretary:	**Mrs Jenny Manthey**
Senior Legal Officers:	**Ms Anita Galeazzi** **Mrs Elise Ho** **Ms Paula Rogers**
Administrative Officer:	**Ms Kahren Giles**

Abbreviations and Glossary

AAUS	Australian Association for Unmanned Systems
AAUS and Liberty Victoria Paper (2015)	AAUS and Liberty Victoria, 'The Use of Drones in Australia: An Agenda for Reform' (May 2015)
ACT Review (2016)	D Stewart, 'Review of ACT Civil Surveillance Regulation' (Report, June 2016)
ALRC	Australian Law Reform Commission
ALRC Discussion Paper No 80 (2014)	Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper No 80 (March 2014)
ALRC Report No 108 (2008)	Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (May 2008)
ALRC Report No 123 (2014)	Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014)
ALRC Report No 22 (1983)	Australian Law Reform Commission, *Privacy*, Report No 22 (1983)
ANPR	automatic number plate recognition
APP entity	A Commonwealth agency (or its contracted service provider), a health service provider, a private sector organisation with an annual turnover of more than $3 million or a business which trades in personal information. An APP entity is required to comply with the *Privacy Act 1988* (Cth).
APPs	Australian Privacy Principles, under the *Privacy Act 1988* (Cth)
Australian Government Issues Paper: Serious Invasion of Privacy (2011)	Australian Government, 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, September 2011)
big data	A data set that is extremely large so that it can be mined for patterns, trends and associations, as in relation to human behaviour online
CASA	Civil Aviation Safety Authority
CCTV	closed circuit television
communication or publication prohibitions	The prohibitions under surveillance devices legislation against the communication or publication of information obtained from the use of a surveillance device
drone	The terms of reference use the term 'drones'. The QDS uses the term 'drone' to refer to any remotely controlled or autonomous aircraft or underwater craft.
Eyes in the Sky Report (2014)	House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy* (July 2014)
Eyes in the Sky Report: Government Response (2016)	Australian Government, 'Australian Government Response to the Standing Committee on Social Policy and Legal Affairs Report: *Eyes in the Sky: Inquiry into drones and the regulation of air safety and privacy*' (December 2016)

GPS	global positioning system
ICT	information and communications technology
IP Act	*Information Privacy Act 2009* (Qld)
IPPs	Information Privacy Principles, under the *Information Privacy Act 2009* (Qld)
Joint Working Group Report (2003)	Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, *Cross-Border Investigative Powers for Law Enforcement*, Report (November 2003)
NSW Parliamentary Committee Report (2016)	Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales* (3 March 2016)
NSWLRC	New South Wales Law Reform Commission
NSWLRC Interim Report No 98 (2001)	New South Wales Law Reform Commission, *Surveillance: an interim report*, Report No 98 (February 2001)
NSWLRC Issues Paper No 12 (1997)	New South Wales Law Reform Commission, *Surveillance*, Issues Paper No 12 (May 1997)
NSWLRC Report No 108 (2005)	New South Wales Law Reform Commission, *Surveillance*, Report No 108 (May 2005)
NZLC	New Zealand Law Commission
NZLC Issues Paper No 14 (2009)	New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies—Review of the Law of Privacy Stage 3*, Issues Paper No 14 (March 2009)
NZLC Report No 113 (2010)	New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies—Review of the Law of Privacy Stage 3*, Report No 113 (January 2010)
NZLC Study Paper No 19 (2008)	New Zealand Law Commission, *Privacy Concepts and Issues—Review of the Law of Privacy Stage 1*, Study Paper No 19 (January 2008)
OAIC	Office of the Australian Information Commissioner
PPRA	*Police Powers and Responsibilities Act 2000* (Qld)
QCAT	Queensland Civil and Administrative Tribunal
QDS (2018)	Queensland Government, *Queensland Drones Strategy* (June 2018)
QDS Consultation Paper (2017)	Queensland Government, 'Queensland Drones Strategy' (Consultation Paper, Department of the Premier and Cabinet, August 2017)
RPA	remotely piloted aircraft
RPAS	remotely piloted aircraft system, including the aircraft and additional components such as attached cameras or sensors, and the control platform

SA Legislative Review Committee Report (2013)	Legislative Review Committee, Parliament of South Australia, *Report of the Legislative Review Committee into Issues Relating to Surveillance Devices* (November 2013)
surveillance devices legislation	Legislation regulating the use of surveillance devices in each Australian jurisdiction, namely: • *Invasion of Privacy Act 1971* (Qld) • *Listening Devices Act 1992* (ACT) • *Surveillance Devices Act 2007* (NSW) and *Surveillance Devices Regulation 2014* (NSW) • *Surveillance Devices Act* (NT) and *Surveillance Devices Regulations* (NT) • *Surveillance Devices Act 2016* (SA) and *Surveillance Devices Regulations 2017* (SA) • *Listening Devices Act 1991* (Tas) and *Listening Devices Regulations 2014* (Tas) • *Surveillance Devices Act 1999* (Vic) and *Surveillance Devices Regulations 2016* (Vic) • *Surveillance Devices Act 1998* (WA) and *Surveillance Devices Regulations 1999* (WA)
UAV	unmanned aerial vehicle
use prohibition	The prohibition under surveillance devices legislation against using (or installing, maintaining or attaching) a surveillance device for certain purposes
VLRC	Victorian Law Reform Commission
VLRC Report No 18 (2010)	Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (June 2010)
VLRC Consultation Paper No 7 (2009)	Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper No 7 (March 2009)
VLRC Occasional Paper (2002)	K Foord, *Defining Privacy*, Victorian Law Reform Commission, Occasional Paper (2002)
VLRC Information Paper (2001)	Victorian Law Reform Commission, *Privacy Law: Options for Reform*, Information Paper (July 2001)

* *Except where otherwise indicated, references to legislation in this Paper are references to Queensland legislation*

Table of Contents

Consultation Questions

The Commission seeks your views on the questions below:

<u>Scope of a new legislative framework</u>

Q-1 What considerations should apply to surveillance that is conducted in a public place?

Q-2 What considerations should apply to surveillance that is conducted overtly or covertly?

Q-3 Should new legislation adopt the existing 'categories' approach used in other jurisdictions and define 'surveillance device' to mean:

- **(a) a listening device;**
- **(b) an optical surveillance device;**
- **(c) a tracking device;**
- **(d) a data surveillance device;**
- **(e) other device (and if so, what should this be)?**

Q-4 If 'yes' to Q-3:

- **(a) how should each category of device be defined?**
- **(b) should each category of device be defined to extend to any particular technologies, such as a program or system?**
- **(c) should 'surveillance device' also include:**
  - **(i) a combination of any two or more of those devices or technologies; or**
  - **(ii) any other device or technology prescribed by regulation?**

Q-5 Alternatively to Q-3, should new legislation adopt a 'technology neutral' approach and define 'surveillance device' to mean, for example, 'any instrument, apparatus, equipment or technology used either alone, or in combination, which is being used to deliberately monitor, observe, overhear, listen to or record an activity; or to determine or monitor the geographical location of a person or an object', or some other definition?

The use of surveillance devices

A prohibition on the use of a surveillance device for particular purposes

Q-6 For what purposes should the use of a surveillance device be prohibited? For example, some or all of:

(a) overhearing, recording, monitoring or listening to a relevant conversation;

(b) observing, monitoring or recording visually a relevant activity;

(c) accessing, tracking, monitoring or recording information that is input into, output from or stored in a computer;

(d) determining the geographical location of a person, vehicle or object;

(e) some other purpose; for example, the collection of biometric data?

Q-7 Should the prohibition in Q-6:

(a) be restricted to intentional or knowing use?

(b) be restricted to private conversations and private activities, or should it extend to some other conversations and activities?

(c) extend to attachment, installation or maintenance of the device?

Exceptions to the prohibition on the use of a surveillance device

Q-8 In what circumstances should a person be permitted to use a surveillance device with consent? What should be the requirements of consent, and should this vary depending upon the particular use or type of device?

Q-9 Should there be a general exception to the prohibition in Q-6 to permit participant monitoring? Why or why not?

Q-10 If 'no' to Q-9, should there be any exceptions that permit participant monitoring in particular circumstances?

Q-11 If 'yes' to Q-10, what should be the particular circumstances for any exceptions and why? For example:

(a) to protect a person's lawful interests;

(b) where it is in the public interest;

(c) where it is consistent with a person's safety or well-being (for example, where there is an imminent threat of violence or property damage, or to protect a child or adult with impaired capacity); or

(d) where it is not intended to communicate or publish to a person who is not a party?

Q-12 Apart from participant monitoring, should there be any exceptions that permit a person to use a surveillance device without consent in particular circumstances?

Q-13 If 'yes' to Q-12, what should be the particular circumstances for any exceptions and why? For example:

(a) to protect a person's lawful interests;

(b) where it is in the public interest; or

(c) where it is consistent with a person's safety or well-being (for example, where there is an imminent threat of violence or property damage, or to protect a child or adult with impaired capacity)?

Q-14 Should there be other circumstances in which the use of a surveillance device is permitted or is not an offence, for example:

(a) for a lawful purpose;

(b) for certain people acting in the course of their occupation, such as media organisations, journalists, private investigators or loss adjusters;

(c) to locate or retrieve a device;

(d) where the use is unintentional; or

(e) in other prescribed circumstances?

If so, what provision should be made for these circumstances, and why?

<u>Communication or publication of information obtained from a surveillance device</u>

Q-15 Should there be a general prohibition on the communication or publication of information obtained through the unlawful use of a surveillance device? Why or why not?

Q-16 If 'no' to Q-15, should the communication or publication of information obtained through the unlawful use of a surveillance device be prohibited in particular circumstances, for example, if the communication of publication is not made:

- **(a) to a party or with the consent of the parties to the private conversation or activity;**
- **(b) in the course of legal proceedings;**
- **(c) to protect the lawful interests of the person making it;**
- **(d) in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;**
- **(e) in the public interest;**
- **(f) in the performance of a duty;**
- **(g) to a person with a reasonable interest in the circumstances;**
- **(h) by a person who obtained knowledge other than by use of the device; or**
- **(i) in any other circumstances?**

Q-17 Should there be a general provision permitting the communication or publication of information obtained through the lawful use of a surveillance device? Why or why not?

Q-18 If 'no' to Q-17, should the communication or publication of information obtained through the lawful use of a surveillance device be permitted in particular circumstances, for example, if the communication or publication is made:

- **(a) to a party or with the consent of the parties to the private conversation or activity;**
- **(b) in the course of legal proceedings;**
- **(c) to protect the lawful interests of the person making it;**
- **(d) in the public interest;**
- **(e) in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;**
- **(f) in the performance of a duty;**
- **(g) to a person with a reasonable interest in the circumstances;**

(h) by a person who obtained knowledge other than by use of the device; or

(i) in any other circumstances?

Q-19 Should any special provision be made in relation to the communication or publication of information obtained through the prohibited or permitted use of a surveillance device:

(a) by a journalist or media organisation;

(b) by a private investigator;

(c) by a loss adjuster; or

(d) in any other circumstances?

If so, what provision should be made and why?

Admissibility of evidence obtained from surveillance device

Q-20 How should the admissibility of evidence, in court proceedings, of information obtained by the unlawful use of a surveillance device be dealt with?

Penalties and remedies

Q-21 Should prohibited use of a surveillance device or prohibited communication or publication of information obtained through the use of a surveillance device be punishable:

(a) as a criminal offence; or

(b) by a civil penalty; or

(c) as either a criminal offence or a civil penalty, as alternatives?

Q-22 How should the liability of a corporation, or a corporate officer, for a contravention by the corporation be dealt with?

Q-23 Should there be power to order the forfeiture of a surveillance device used in a contravention of the legislation, or of a report or record of information obtained by the use of a surveillance device in a contravention of the legislation?

Q-24 Is it necessary for the legislation to include any other ancillary prohibitions, for example, to deal with:

(a) the possession of records obtained from the prohibited use of surveillance devices?

(a) the possession, manufacture, supply or advertising of surveillance devices?

(b) the use of surveillance devices to intimidate, harass or hinder a person?

Q-25 Should there be a right to bring a civil proceeding in respect of a contravention of the prohibited use of a surveillance device or the prohibited communication or publication of information obtained through the use of a surveillance device?

Q-26 If yes to Q-25, what relief should be available to a plaintiff in a civil proceeding, for example:

(a) an order that the contravener is prohibited from conduct (for example, from using a surveillance device) or must do something (for example, remove a surveillance device)?

(b) a declaration (that the conduct was unlawful or that the unlawful conduct breached the person's privacy)?

(c) an order for monetary compensation (for any loss or damage or up to any particular amount)?

(d) other relief?

Q-27 If yes to Q-26(a), should breach of a prohibitory or mandatory order be a criminal offence or dealt with as a contempt or by some other procedure?

<u>Enforcement and regulatory powers</u>

Q-28 Should there be an independent regulator and, if so, what entity should this be?

Q-29 What regulatory and compliance functions or powers should be conferred on an independent regulator or otherwise provided for under the legislation, for example:

(a) conciliation or mediation of complaints about breaches of the legislation;

(b) appointment of inspectors to investigate or monitor compliance with the legislation;

(c) the issue of compliance notices;

(d) starting civil penalty proceedings;

(e) education and best practice guidance and advice about the legislation;

(f) research, monitoring and reporting of matters relevant to the legislation?

Part 1: Introduction

Background to the review

[1.1] With the development of new and emerging surveillance technologies, surveillance devices have become increasingly affordable, available and sophisticated. However, surveillance brings with it the potential to interfere with or intrude on an individual's privacy.

[1.2] In Queensland, the use of surveillance devices for civil surveillance is not comprehensively regulated. The *Invasion of Privacy Act 1971* regulates only the use of listening devices. Other laws of more general application offer only limited privacy protection.

[1.3] In most other Australian jurisdictions, surveillance devices legislation regulates the use of listening devices, optical surveillance devices, tracking devices and data surveillance devices.

The Queensland Drones Strategy

[1.4] In June 2018, the Queensland Government released the Queensland Drones Strategy (the 'QDS').[1] The QDS is designed 'to build on [Queensland's] strengths and [to] leverage the State's innovation success to take advantage of new and emerging opportunities' in the drones industry.

[1.5] Whilst noting the potential of drone technology to 'enhance peoples' lives and support … communities', the QDS also had regard to concerns about the adequacy of Queensland's legislation to protect the privacy of individuals with the emergence of new technology. To address those concerns, the QDS recommended that the Queensland Government refer to the Queensland Law Reform Commission (the 'Commission') the question of 'whether Queensland's legislation adequately protects individuals' privacy in the context of modern and emerging technologies'.[2]

The terms of reference

[1.6] On 24 July 2018, the Attorney-General referred to the Commission for review 'the issue of modernising Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies'.

[1.7] The Commission's terms of reference require it to 'recommend whether Queensland should consider legislation to appropriately protect the privacy of individuals in the context of civil surveillance technologies', including to:[3]

---

1 Queensland Government, *Queensland Drones Strategy* (June 2018). The objectives of the QDS are to attract national and international investment, increase industry and workforce capability, increase research and development, support community-friendly drone policies and improve government service delivery: 4–5.

2 Ibid 3, 31, 40.

3 The terms of reference are set out in full in Appendix A.

1. regulate the use of surveillance devices (such as listening devices, optical surveillance devices, tracking devices and data surveillance devices) and the use of emerging surveillance device technologies (including remotely piloted aircraft (or 'drones') fitted with surveillance devices) to appropriately protect the privacy of individuals;

2. regulate the communication or publication of information derived from surveillance devices;

3. provide for offences relating to the unlawful use of surveillance devices and the unlawful communication or publication of information derived from a surveillance device;

4. provide appropriate regulatory powers and enforcement mechanisms in relation to the use of surveillance devices;

5. provide appropriate penalties and remedies; and

6. otherwise appropriately protect the privacy of individuals in relation to the use of surveillance devices.

[1.8] The terms of reference exclude from the review Queensland's existing law regulating the use of surveillance devices for State law enforcement purposes.[4] Accordingly, chapter 13 of the *Police Powers and Responsibilities Act 2000* (which regulates the use of surveillance devices by police) and chapter 3 part 6 of the *Crime and Corruption Act 2001* (which regulates the use of surveillance devices by an authorised officer of the Crime and Corruption Commission) are outside the scope of the review.

[1.9] The issue of whether there should be a legislative framework to regulate the surveillance of workers by employers using surveillance devices is also excluded from the review.[5] This issue has been referred to the Commission for review under separate terms of reference.[6]

[1.10] On 7 December 2018, the Attorney-General amended the terms of reference, at the Commission's request, to ask the Commission to prepare draft legislation based on its recommendations and, accordingly, to extend the reporting date from 1 July 2019 to 31 October 2019.[7]

Civil surveillance law reform reviews in other jurisdictions

[1.11] There have been a number of recent law reform reviews and other inquiries which, relevantly to this review, have considered surveillance regulation in Australia.

[1.12] A brief overview of those reviews and inquiries is contained in Appendix D.

---

4 See terms of reference, para E.

5 See terms of reference, para F.

6 The terms of reference for the review of Queensland's laws relating to workplace surveillance are available on the Commission's website at <https://www.qlrc.qld.gov.au/__data/assets/pdf_file/0005/589514/workplace-surveillance-amended-tor.pdf>.

7 Letter from the Attorney-General and Minister for Justice, Leader of the House, the Hon Yvette D'Ath MP, to the Chair of the Queensland Law Reform Commission, the Hon Justice David Jackson, dated 7 December 2018.

The structure of this paper

[1.13] This paper is divided into three parts.

[1.14] Part 1 introduces the review and the objectives of the terms of reference.

[1.15] Part 2 provides an overview of privacy, surveillance, current and emerging surveillance devices and their uses, privacy implications of surveillance technologies, relevant community attitudes and the current legal framework for the regulation of surveillance.

[1.16] Part 3 outlines the key issues raised by the terms of reference, including the scope of a new legislative framework, regulating the use of surveillance devices and the communication and publication of information obtained from their use, the provision of appropriate penalties and remedies and other matters relating to the regulation and enforcement of surveillance devices legislation in Queensland.

[1.17] The questions posed in the paper are set out in full on pages iii–ix above. Responses to the questions will inform the development of the Commission's recommendations for proposed new legislation in relation to surveillance devices.

Making a submission

[1.18] The Commission invites written submissions in response to the questions in this paper by **31 January 2019**.

[1.19] Information about how to make a submission is set out at the beginning of the paper.

Part 2: Background

Privacy

[2.1] The concept of individual privacy is complex, multifaceted and difficult to define. It may mean different things to different people and in different contexts. As society changes, expectations of privacy may also change.[8]

[2.2] Privacy may be described in a general way as the interests a person has in controlling what others know about them, in being left alone and in being free from interference or intrusion.[9] Privacy has long been expressed as the 'right to be let alone'.[10]

[2.3] The *Oxford English Dictionary* defines 'privacy' as:[11]

> The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.

[2.4] In simple terms, privacy can be understood to involve 'private spheres',[12] 'personal spaces'[13] or 'boundaries'.[14] As Privacy International explains:[15]

> Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information.

---

8 There is a considerable literature on privacy, but no fixed definition. It is often observed that a precise and exhaustive definition of privacy is difficult: see, eg, D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) *Melbourne University Law Review* 131, 135. See generally JL Mills, *Privacy: The Lost Right* (Oxford University Press, 2008) 13–22.

9 See, eg, International Association of Privacy Professionals ('IAPP'), *What does privacy mean?* (2018) <https://iapp.org/about/what-is-privacy/>.

10 This description appears in an article by SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193, 195, referring to TM Cooley, *A Treatise on the Law of Torts: or the Wrongs which Arise Independent of Contract* (Callaghan, 2nd ed, 1888) 29. Warren and Brandeis were concerned with the need to protect individuals' privacy 'from invasion' and public disclosure 'either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds': 206.

11 *Oxford English Dictionary* (Oxford University Press, online, 2018). The *Macquarie Dictionary* contains a similar definition.

12 See, eg, JA Cannataci et al, 'Privacy, free expression and transparency: Redefining their new boundaries in the digital age' (Report, UNESCO, 2016) [3.1].

13 See, eg, R Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Xamax Consultancy Pty Ltd, 15 August 1997, revised 24 July 2016) <http://www.rogerclarke.com/DV/Intro.html>.

14 See, eg, VLRC Occasional Paper (2002) 5; S Wong, 'The concept, value and right of privacy' (1996) 3 *UCL Jurisprudence Review* 165, 167–9.

15 Privacy International, *What is privacy?* <https://privacyinternational.org/explainer/56/what-privacy>.

[2.5] Privacy does not necessarily imply secrecy; rather, it is the interest individuals have in controlling who has access to different aspects of their lives and when.[16]

[2.6] Discussions of privacy sometimes distinguish between what is 'private' and what is 'public', but this can be misleading since privacy can still have a role to play in public places.[17] It has been observed that:[18]

> Protection of privacy is … not dependent on classification of physical spaces as public or private. It provides a choice over how, as individuals, we interact with others, even in publicly accessible locations.

[2.7] Individual privacy is comprised of many related and overlapping interests or dimensions. Most commonly, these are identified as:[19]

- *Privacy of the person* or *bodily privacy*—the interest in freedom from interference with an individual's physical person and bodily integrity, including from direct and indirect physical intrusions. It may also include psychological intrusion.[20]
- *Privacy of personal space* or *territorial privacy*—the interest in limiting intrusion into personal spaces, including in the home, workplace and in public. This concerns a person's sense of personal safety and dignity as well as their property rights.
- *Privacy of personal communications* or *communications and surveillance privacy*—the interest in freedom from interference with personal communications, including interception, recording, monitoring or surveillance.
- *Privacy of personal information* or *information/data privacy*—the interest in controlling access to, use and disclosure of information about the person, including images and information 'derived from analysis' of other data.[21]

[2.8] Other privacy interests include:

- *Privacy of personal behaviour* or *behavioural privacy*—the interest in freedom from undue observation of or interference with a person's activities,

---

16 See, eg, LP Francis and JG Francis, *Privacy: What Everyone Needs to Know* (Oxford University Press, 2017) 15–16.

17 'There is no bright line which can be drawn between what is private and what is not': *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [42] (Gleeson CJ).

18 ACT Review (2016) [3.7].

19 See, eg, IAPP, *Glossary of Privacy Terms* (2018) (definitions of 'privacy, four classes of' and related definitions) <https://iapp.org/resources/glossary/>. '[T]hese are not hard and fast categories': see Evidence to Standing Committee on Law and Justice, Parliament of New South Wales, Sydney, 16 November 2015, 40 (Anna Johnston, Director, Salinger Privacy).

20 See, eg, VLRC Information Paper (2001) [2.1], [2.19].

21 J Waldo, HS Lin and LI Millett (eds), *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, 2007) 22.

movements, associations and preferences, including sensitive matters such as sexual preferences, political activities and religious practices.[22]

- *Privacy of personal experience*—referring to concerns about the storage and use of collected data about an individual's personal experiences, including what they read and view and who they interact and associate with.[23]
- *Locational privacy* or *tracking privacy*—the interest in controlling the extent to which information about a person's current or past location(s) is accessed and used by others.[24]
- *Privacy of thoughts and feelings*—the interest a person has in not sharing their thoughts or feelings and not having them revealed to others.[25]
- *Privacy of attention*—the ability to exclude intrusions that force a person to direct attention to them, rather than to matters of their own choosing.[26]
- *Privacy through anonymity*—the interest in choosing to be and remain anonymous, for example, when entering into transactions with organisations.[27]

[2.9] Privacy has been characterised variously as a value, an interest, a claim and, in some circumstances, a right. A right to privacy is recognised under international human rights law, in the Human Rights Bill 2018 and in the human rights statutes of some other jurisdictions.[28]

[2.10] Privacy is recognised as a fundamental value that underpins human dignity in many activities, such as:[29]

- meaningful and satisfying interpersonal relationships, including intimate and family relationships;
- freedom of speech, thought and self-expression;
- freedom of movement and association;

---

22 See, eg, R Clarke, 'The regulation of civilian drones' impacts on behavioural privacy' (2014) 30(3) *Computer Law & Security Review* 286, [2.2].

23 See, eg, Clarke, above n 22, [2.2]. A related privacy interest is 'privacy of association (including group privacy)' which is concerned with the freedom to associate with others without being monitored: M Friedewald, RL Finn and D Wright, 'Seven types of privacy' (2013) <https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy>.

24 See, eg, K Michael and R Clarke, 'Location and Tracking of Mobile Devices: Uberveillance Stalks the Streets' (2013) 29(3) *Computer Law & Security Review* 216, [5.1].

25 Friedewald, Finn and Wright, above n 23.

26 See, eg, SI Benn, 'The Protection and Limitation of Privacy Part I' (1978) 52(11) *Australian Law Journal* 601, 608–9.

27 See, eg, VLRC Occasional Paper (2002) 14–15; Waldo, Lin and Millet, above n 21, [1.5.3].

28 See [2.100]–[2.102] and Appendix E.

29 ALRC Report No 123 (2014) [2.6]. Privacy is 'not less valuable or deserving of legal protection simply because it is hard to define': [2.9]; and see NSW Parliamentary Committee Report (2016) [2.7]–[2.8]; Mills, above n 8, 26.

- engagement in the democratic process;
- freedom to engage in secure financial transactions;
- freedom to pursue intellectual, cultural, artistic, property and physical interests; and
- freedom from undue interference or harm by others.

[2.11] Privacy is important to individual autonomy and dignity;[30] as well as to other individual freedoms in which society has an interest:[31]

> Privacy is an integral part of the amalgamation of values that define a healthy society. Specifically, privacy promotes *individuality*, *intimacy* and *liberty*. … The loss of privacy, therefore, not only is a loss to each of us as individuals, but also impairs creativity in art, science, and living. The loss of privacy can hurt each of us and all of us. (emphasis in original)

[2.12] An expectation of privacy is a core element of modern liberal democracy. It derives from the liberal notion of a personal (or private) sphere in which individuals, as long as they do not harm others, are free to act without government interference.[32] Accordingly, it has been said that:[33]

> it is in the interests of citizens not to be observed by the state when pursuing lawful personal projects. It is in the interests of citizens to have portions of life and of civil society that operate independently of the state.

[2.13] A 'reasonable expectation of privacy' is the critical measure used to determine the acceptable limits of actions, such as surveillance, that might infringe upon privacy, including in public places. Whether an expectation of privacy is reasonable in the circumstances is likely to depend on factors such as:[34]

- location (for example, a public park and a public bathroom would be associated with different expectations, and there would also be different expectations for private places, such as a person's home);
- the type of activity that is being engaged in;

---

30 See, eg, VLRC Occasional Paper (2002) 17–20, 22. This includes the 'rights' of individuals not to be treated as a 'thing' and to establish and develop relationships with others: 22.

31 Mills, above n 8, 26–7. Privacy can be conceived as a public and collective value: see, eg, ALRC Report No 123 (2014) [2.16] ff; VLRC Occasional Paper (2002) 39–40.

32 O Raban, 'Capitalism, Liberalism, and the Right to Privacy' (2012) 86 *Tulane Law Review* 1243, 1247. This has been conceptualised as 'private choice' or 'decisional privacy', and is said to derive (like other liberal ideals) from 17th and 18th century political ideas about individual freedom and the social contract. One strand of liberal theory contends that it has its origins in a distinction in classical antiquity between the 'public' sphere of the city-state and the 'private' sphere of the household, although this has been debated: see generally, eg, AL Allen, 'Coercing Privacy' (1999) 40(3) *William and Mary Law Review* 723, 724–5; A Tessitore, 'Review Essay: Aristotle & Modern Liberalism' (1993) (25)(4) *Polity* 647.

33 T Sorell and J Guelke, 'Chapter 3: Liberal Democratic Regulation and Technological Advance' in R Brownsword, E Scotford and K Yeung (eds), *The Oxford Handbook of Law, Regulation, and Technology* (Oxford University Press, 2017) 90, 90–91.

34 See, eg, NSWLRC Interim Report No 98 (2001) [1.13], [4.41]–[4.43]; VLRC Report No 18 (2010) [5.11]–[5.17]. The NSWLRC and the VLRC incorporated the concept of a reasonable expectation of privacy into their principles regulating 'overt surveillance' and surveillance in public places, respectively.

- a person's identity (for example, if they are a public figure), behaviour (for example, if they are deliberately seeking attention) or particular vulnerability (for example, if they are ill); and
- if surveillance is used:
  - whether the person is notified of, or consents to, the use of the surveillance;
  - the purpose of the surveillance; and
  - whether the surveillance used is appropriate in the circumstances (for example, a business may require visual but not audio surveillance).

[2.14] Privacy is not an absolute interest or right, but exists in relationship with other interests.[35] Some of these are identified as 'complementary' to privacy, such as confidentiality, reputation and non-discrimination.[36] A wide range of other interests are identified as potentially conflicting with privacy, including:[37]

- freedom of speech, including the freedom of the media and the implied constitutional freedom of political communication;
- freedom of artistic and creative expression and innovation in the digital era;
- the public's right to be informed on matters of public importance, [in a timely way];
- public access to information and accurate historical records;
- the proper administration of government and matters affecting the public or members of the public;
- the promotion of open justice;
- national security and safety;
- the prevention and detection of criminal and fraudulent activity and the apprehension of criminals;
- the effective delivery of essential and emergency services in the community;
- the protection of vulnerable persons in the community;
- the right to be free from violence, including family violence;
- national economic development and participation in the global digital economy;
- the social and economic value of analysing 'big data';

35 See generally the discussion of 'tensions' and 'trade-offs' in Waldo, Lin and Millet, above n 21, 22–5.

36 See ALRC Report No 22 (1983) vol 1, [68]–[74].

37 ALRC Report No 123 (2014) [2.22], citing various submissions to its review.

- the free flow of information and the right of business to achieve its objectives efficiently; and
- the value of individuals being enabled to engage in digital communications and electronic financial and commercial transactions. (notes omitted)

[2.15] The protection of individual privacy must be balanced against other public interests. Notably, this includes freedom of expression and opinion which, like privacy, is recognised as a fundamental human right.[38]

[2.16] Although there is a recognised tension between privacy and freedom of expression, they are not mutually exclusive; the freedom to communicate with others, to create and innovate can be enhanced through confidence in the privacy of one's communications and activities.[39]

[2.17] Relevantly, the ALRC nominated the following three guiding principles for privacy reform:[40]

- Privacy is a fundamental value worthy of legal protection.
- There is a public interest in protecting privacy.
- Privacy should be balanced with other important interests.

[2.18] Consistency with international standards, national harmonisation, clarity and certainty, accessibility, shared responsibility, and adaptability to technological change have also been recognised as important factors in privacy protection.[41]

[2.19] The concept of privacy has developed alongside the advent of new technologies and modes of social interaction.[42] The proliferation of information and communications technologies ('ICTs') has been accompanied by concerns about information and data privacy, which has been the primary focus of most privacy regulation.[43]

---

38 In the context of arts 17, 19(2) of the ICCPR, see Appendix E.

39 See, eg, NSWLRC Report No 108 (2005) [3.28]. See also JE Cohen, 'What Privacy is For' (2013) 126(7) *Harvard Law Review* 1904, 1905–06: 'a society that values innovation ignores privacy at its peril, for privacy also shelters the processes of play and experimentation from which innovation emerges'.

40 ALRC Report No 123 (2014) ch 2 'Guiding Principles', principles 1–3.

41 Ibid, principles 4–9.

42 See, eg, T Mendel et al, 'Global Survey on Internet Privacy and Freedom of Expression' (UNESCO Series on Internet Freedom, 2012) 9.

43 See the discussion of information privacy legislation at [2.103] ff below. Especially in the context of data surveillance, there is an overlap between the practice of surveillance and information or data privacy. Information privacy laws, including the *Privacy Act 1988* (Cth), regulate the collection, storage, use and disposal of personal information held by particular entities. Surveillance devices legislation, in contrast, regulates the use of surveillance devices and the communication or publication of information obtained from that use. The focus of this review is surveillance devices legislation. As to this overlap and distinction, see generally NSWLRC, Interim Report No 98 (2001) [2.68] ff; VLRC, Consultation Paper No & (2009) [1.35] ff.

[2.20] The emergence of new surveillance technologies has also brought with it renewed concerns about privacy. Most, if not all, of the privacy interests noted above have the potential to be impacted by surveillance.[44]

44 See [2.26] ff, [2.37] ff below.

Surveillance

[2.21] The term 'surveillance' comes from the French word 'surveiller', meaning to 'watch over'. It commonly means:[45]

> 1. watch kept over a person, etc., especially over a suspect, a prisoner, or the like.
>
> 2. a general watch maintained over an area or location, usually by devices such as cameras, recorders, etc.
>
> 3. supervision or superintendence.

[2.22] Surveillance in the broad sense of 'watching over' is 'an everyday practice in which human beings engage routinely, often unthinkingly'.[46] However, the term also has a more specific usage, 'referring to some focused and purposive attention to objects, data, or persons'.[47] In this sense, surveillance is context-specific and is 'always hinged to some specific purposes':[48]

> On the one hand, then, surveillance is a set of practices, while, on the other, it connects with purposes.

[2.23] In considering reforms to surveillance devices legislation, a number of law reform commissions and other government bodies have examined the meaning of 'surveillance'. They each considered that 'surveillance' involves the deliberate monitoring of a person, a group of people, a place or an object for some purpose, usually to obtain certain information about the person who is the subject of the surveillance. It may occur on a single occasion or be a systematic activity.[49]

[2.24] Surveillance may be overt or covert, or a combination of both. Surveillance may be described as 'overt' where the subject of surveillance is aware that surveillance is occurring, or the surveillance device is not concealed, for example, CCTV cameras in a bank. Surveillance may be described as 'covert' where the subject of surveillance is not aware that surveillance is occurring, or the surveillance device is concealed, for example, a listening device secreted in a person's car.[50]

---

45 *Macquarie Dictionary* (Macmillan Publishers Australia, online, 2018), 'Surveillance'.

46 D Lyon, 'Surveillance, power, and everyday life' in C Avgerou et al (eds), *The Oxford Handbook of Information and Communication Technologies* (Oxford University Press, 2009) 449, 450.

47 Ibid.

48 D Lyon, *Surveillance Studies: An Overview* (Polity Press, 2007) 15.

49 ALRC Report No 108 (2008) vol 1, [9.89]; VLRC Report No 18 (2010) [1.11]–[1.14]; VLRC Consultation Paper No 7 (2009) [1.13]–[1.15]; NSWLRC Report No 108 (2005) [1.8]; ACT Review (2016) [3.1]. See also Office of the Victorian Information Commissioner (formerly the Commissioner for Privacy and Data Protection), *Guidelines to Surveillance and Privacy in the Victorian Public Sector* (May 2017) 8, in which it was stated that:

> Surveillance is typically an intentional act done for a specific purpose, rather than an incidental consequence of some other activity.

50 NSWLRC Interim Report No 98 (2001) [2.78]–[2.79], [2.86]–[2.88], pts 2, 3; NSWLRC Report No 108 (2005) [3.12]–[3.21], chs 4 and 5. The NSWLRC noted that the policy issues behind both overt and covert surveillance are different, though the technology used may be identical, and acknowledged that the distinction between the two types of surveillance is not always clear: NSWLRC Issues Paper No 12 (1997) [2.3].

[2.25] Surveillance is commonly thought of in terms of law enforcement, including the investigation, detection and prevention of crime by police.[51] However, civil surveillance is conducted by numerous agencies, organisations, businesses and individuals for a variety of purposes, including for public health and safety, emergency response, traffic management, crowd control, the protection of personal safety and private property, marketing and research or workplace monitoring.[52]

Categories of surveillance

[2.26] Different forms of surveillance capture different types of information. Common categories include:[53]

- *Listening* or *audio surveillance*—listening to or recording sounds, usually conversations. This may be done with the assistance of aids to enhance human hearing, such as directional microphones, voice recorders or 'bugs'. It may also include intercepting communications, such as phone conversations or voice communications over the internet.
- *Optical* or *visual surveillance*—watching a person or place. It may be undertaken with the assistance of aids to enhance human vision, such as telescopes or infra-red binoculars. It may also include the use of devices that can record or stream images, such as cameras, video recorders or CCTV.
- *Data surveillance*—the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. It may include surveillance of a person's electronic records, including those relating to credit cards or loyalty cards, email communications or computer usage and internet activities using tools such as cookies, keystroke monitoring or spyware.
- *Tracking* or *location surveillance*—the observation or recording of a target's location. Location data may capture the location of a person or object at a point in time or monitor a person's movements in real-time. It may also involve predictive tracking or retrospective tracking, based on the data trail of a person's movements. Examples of location and tracking devices include global positioning system ('GPS') and satellite technology tracking, radio frequency identification ('RFID'), and automatic number plate recognition ('ANPR').
- *Biometric surveillance*—the collection or recording of biological samples and physical or behavioural characteristics, usually for the purpose of identifying an individual. This may include fingerprints, cheek swabs, iris scans and blood

---

51 The use of surveillance devices for State law enforcement purposes is excluded from this review: see terms of reference, para E.

52 Workplace surveillance is excluded from this review: see terms of reference, para F. It is the subject of a separate review that has been referred to the Commission.

53 See, eg, R Clarke, *A Framework for Surveillance Analysis* (Xamax Consultancy Pty Ltd, 2012) <http://www.rogerclarke.com/DV/FSA.html>; Clarke, above n 13; Michael and Clarke, above n 24, [3]; VLRC Consultation Paper No 7 (2009) [1.13]–[1.18].

or urine samples. Other examples include face or voice recognition or gait analysis technology.

Surveillance technologies

[2.27] Surveillance technologies have become increasingly sophisticated, with advanced capabilities and internet connectivity. At the same time, they are becoming smaller, less expensive, more accessible and widely available.[54] It is anticipated that surveillance devices will become increasingly autonomous, intelligent and connected in the future, and that the trend towards convergence will continue.[55]

[2.28] In the past, surveillance 'was of necessity a human-intensive activity, involving watching and listening'.[56] Surveillance devices primarily enhanced human hearing (for example, directional microphones or 'bugs') or seeing (for example, binoculars and cameras).[57] Their use was limited 'by the high cost of the technology and by physical capabilities'.[58] It was also limited in that 'information tended to stay local, compartmentalised, unshared and was often unrecorded, or if kept, difficult to retrieve and analyse in depth'.[59]

[2.29] However, technological advancements, including in relation to computers, sensors, data storage, location tracking and networking, have significantly contributed to the development and proliferation of new surveillance capabilities.[60] In addition, the proliferation of digital data,[61] combined with the increasing capacity to

---

54 See, eg, AAUS and Liberty Victoria Paper (2015) 8–9; VLRC Consultation Paper No 7 (2009) [2.13]–[2.16].

55 The World Economic Forum stated that we are now in the 'fourth industrial revolution', which builds on the digital revolution and will be characterised by 'cyber-physical systems' and 'a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres': K Schwab, 'The Fourth Industrial Revolution: What it means, how to respond' (14 Jan 2016) World Economic Forum <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>. See also N Davis, 'What is the fourth industrial revolution?' (19 Jan 2016), World Economic Forum <https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/>.

56 R Clarke, *What drones inherit from their ancestors* (Xamax Consultancy Pty Ltd, 2013–14) <http://www.rogerclarke.com/Drones-I.html>.

57 Ibid.

58 AAUS and Liberty Victoria Paper (2015) 9. For example, they required:

> physical proximity (for example, requiring the user to press a button to activate a device, such as a point-and-click camera); and
>
> physical access, usually in order to install a surveillance device (for example, a microphone or camera) which cannot easily be done on private property.

59 K Ball, K Haggerty and D Lyon, *Routledge Handbook of Surveillance Studies* (Routledge, 2012) xxv.

60 See, eg, European Group on Ethics in Science and New Technologies, *Ethics of Security and Surveillance Technologies*, Opinion No 28 (20 May 2014) ch 1; The National Academies of Sciences Engineering and Medicine, *Engaging Privacy and Information Technology in a Digital Age* (2007) ch 3; NZLC Study Paper No 19 (2008) ch 6; VLRC Consultation Paper No 7 (2009) ch 2.

61 According to DOMO, in 2017, 90 per cent of all the data on the internet was created in the previous two years (which is 2.5 quintillion bytes of data per day): DOMO, 'Data Never Sleeps 5.0' (2017) <https://www.domo.com/learn/data-never-sleeps-5>. Internet users have risen from 2.5 billion in 2012 to 3.8 billion in 2017. By 2020, it is estimated that for every person on earth, 1.7 MB of data will be created every second: DOMO, 'Data Never Sleeps 6.0' (2018) <https://www.domo.com/learn/data-never-sleeps-6>.

store, analyse and aggregate or combine that data, has given rise to new forms of data surveillance, including data mining and data profiling of 'big data'.[62]

[2.30] Surveillance devices include technologies or devices that are developed specifically for surveillance purposes, as well as those that are capable of being used for surveillance.

[2.31] A smartphone is an obvious example of an everyday device that is capable of being used as a surveillance device because of its camera and video and audio recording capabilities, GPS and location tracking software, and internet connectivity.

[2.32] Drones are another example of an emerging technology capable of being used for surveillance, as they provide 'new capabilities for recording images, videos and sounds'.[63] The AAUS and Liberty Victoria observed that:[64]

> It is only in recent years that unmanned systems [drones] have started to fall within the reach of individual consumers from a financial, logistical and technological perspective. Just years ago, a small unmanned system would have cost thousands of dollars; today, for less than $250 Australian consumers can purchase an unmanned system featuring a high-definition camera, microphone and ultrasound altimeter, that can be remotely controlled via a mobile phone or tablet. As the technology continues to mature and prices continue to decrease, these systems are likely to proliferate.

[2.33] Aerial drones are already used in a variety of civilian applications. For example, drones are being used in the arts for cinematography and photography, by real estate agents to take aerial photographs of properties, by lifeguards to patrol beaches, by farmers to monitor crops and livestock, by government agencies to survey lands and conduct building and infrastructure inspections, and by scientists to monitor habitats and wildlife populations or tidal and weather patterns.[65]

---

62 'Data mining' refers to the application of statistical techniques and programming algorithms to analyse data for both known and previously unknown data patterns. 'Data profiling' is the process of compiling information about a particular individual, or group, in order to generate a profile (that is, an analysis of their traits and characteristics from the data available). Pattern recognition technology may also be used for predictive analysis. See generally, *Macquarie Dictionary* (Macmillan Publishers Australia, online, 2018) 'Data-mining'; JH Ziegeldorf, OG Morchon and K Wehrle, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7(12) *Security and Communications Networks* 2728, [4.3]; R Clarke, *Dataveillance Regulation: A Research Framework* (Xamax Consultancy Pty Ltd, 2017) <http://www.rogerclarke.com/DV/DVR.html> and the sources cited there.

63 QDS (2018) 9, 31. The term 'drone' is commonly used to refer to any unmanned craft that is remotely controlled or autonomously piloted. They are also referred to variously as a remotely piloted aircraft ('RPA'), remotely piloted aircraft system ('RPAS'), unmanned aerial vehicle ('UAV'), unmanned aerial system ('UAS'), unmanned underwater vehicle ('UUV') or autonomous underwater vehicle ('AUV').

64 AAUS and Liberty Victoria Paper (2015) 8–9.

65 See ibid 6, 8; QDS (2018); World of Drones Congress, Brisbane, 9–10 August 2018 <https://www.worldofdrones.com.au/program>; European Group on Ethics in Science and New Technologies, above n 60, 52–5.

[2.34] Another emerging technology is 'smart CCTV', which combines CCTV cameras with facial recognition software and artificial intelligence (including predictive systems to identify different behaviours):[66]

> The latest research in automated surveillance is concerned with recognition of individuals and their intentions. Facial recognition software can automatically analyse video, pick a face from a crowd and identify the individual by comparison with a database of known faces. The person can then be tracked from camera to camera across wide geographical areas without any human intervention. Automated cameras can also be programmed to identify 'suspicious behaviour' or 'threats' eg. an individual entering a restricted access zone or unattended luggage in an airport. (note omitted)

[2.35] CCTV with facial recognition technology is already being used for security and policing purposes.[67]

[2.36] CCTV cameras in public places typically record video only. An emerging issue is the potential use of CCTV in public spaces that also record audio.[68]

---

66 European Group on Ethics in Science and New Technologies, above n 60, 29. See further J Vincent, 'Artificial intelligence is going to supercharge surveillance' (23 January 2018) *The Verge* <https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security>; A Bigdeli, B Lovell and S Mau, 'You, yes you: welcome to the world of advanced surveillance', *The Conversation* (23 May 2011) <https://theconversation.com/you-yes-you-welcome-to-the-world-of-advanced-surveillance-830>.

67 Facial recognition software was reportedly used in Queensland for security during the Commonwealth Games: G Roberts, 'Commonwealth Games facial recognition software to stay, but when will it be used? The Queensland Government won't say', *ABC News* (online), 19 April 2018 <http://www.abc.net.au/news/2018-04-19/qldrefuse-to-say-how-it-will-use-new-facial-recognition-software/9677156>. The use of live facial recognition technology is currently being trialled by the London Metropolitan Police Service: London Policing Ethics Panel, *Interim Report on Live Facial Recognition* (July 2018). The Chinese Government is also reportedly using live facial recognition technology on CCTV cameras: M Carney, 'Leave no dark corner', *ABC News* (online), 19 September 2018 <http://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>. In addition, police in China are reportedly using glasses with facial recognition technology for identity verification and to identify criminal suspects: B Fu, 'Police in China are wearing facial recognition glasses', *ABC News* (online), 8 February 2018 <https://abcnews.go.com/International/police-china-wearing-facial-recognition-glasses/story?id=52931801>.

68 See, eg, Office of the Information Commissioner (Qld), 'Moreton Bay Regional Council's use of upgraded CCTV cameras with audio recording capability' (Media Release, 8 February 2017) <https://www.oic.qld.gov.au/information-for/media/moreton-bay-regional-councils-use-of-upgraded-cctv-cameras-with-audio-recording-capability-8-february-2017>.

Privacy implications of surveillance technologies

[2.37] Civil surveillance technologies are used for a range of legitimate purposes.[69] It is also possible, however, for surveillance technologies to be used for improper and harmful purposes such as theft, stalking, harassment, bullying, peeping or prying.

[2.38] Whatever the purpose, surveillance technologies have the potential to impact on individual privacy.[70]

[2.39] General concerns about surveillance include the 'chilling effect' that it can have on freedom of expression and action: if people know or suspect that they are being surveilled, they may self-censor and inhibit their behaviour.[71] Other concerns include the possibility that surveillance may be used when it is disproportionate to or ineffective for its purpose, and that it may lead to discrimination or social exclusion for marginalised or stigmatised members of the community. Many of these concerns relate especially to surveillance in public places or by public authorities.[72]

[2.40] Surveillance also has the potential for more direct impacts on individual privacy. The nature of current and emerging civil surveillance technologies poses a number of specific privacy challenges.[73]

[2.41] The enhanced capabilities of surveillance technologies allow for more intrusive surveillance. Surveillance technologies enable access to previously out of reach places and different forms of data. For example: cameras mounted on aerial drones can 'peer' over fences; infra-red sensors can 'see' through walls; smart devices can be used by outsiders to remotely 'listen in' to people in their homes; cameras with higher resolution and improved zoom capacity can capture more detailed images from greater distances; and new forms of information, such as GPS location information, can be accessed and tracked over time.

[2.42] Increasing sophistication of surveillance technologies also allows for more covert surveillance. Many surveillance technologies can be activated and controlled remotely without the subject's knowledge. Others may be too small or unobtrusive to be noticed. Many are mobile.

---

69 See, eg, [2.25], [2.33] above.

70 See generally, Mills, above n 8, 29 ff. See also, eg, R Clarke, 'Managing Drones' Privacy and Civil Liberties Impacts' (Xamax Consultancy Pty Ltd, 21 July 2014) <http://www.rogerclarke.com/SOS/Drones-PCLI.html>; Ziegeldorf, Morchon and Wehrle, above n 62, [4].

Technologies can also be used to address privacy concerns through the adoption of 'privacy by design' principles and the use of 'privacy-enhancing technologies': see, eg, European Union Agency for Network and Information Security (ENISA), *Privacy by Design* and *Privacy enhancing technologies* (2018) from the links at <https://www.enisa.europa.eu/topics/data-protection>.

71 See, eg, DJ Solove, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477, 493-5; B Gogarty, 'Unmanned Vehicles, Surveillance Saturation and Prisons of the Mind' (2011) 21(2) *Journal of Law, Information and Science* 180, 188; ALRC Report No 123 (2014) [14.12]–[14.13].

72 See, eg, VLRC Report No 18 (2010) [4.35]–[4.41].

73 See generally GT Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) 1(1) *Surveillance & Society* 9, 15, table 1 as to the various ways in which new and emerging surveillance technologies differ from traditional methods of surveillance.

[2.43] The affordability and accessibility of surveillance technologies also allows for the decentralised and more widespread use of surveillance. Surveillance technologies are increasingly accessible to private individuals, groups and businesses. For example, 88% of Australians now own a smartphone[74] and CASA has estimated there are more than 100 000 privately operated drones in Australia,[75] many of which may carry surveillance devices. Surveillance has also become more common in public and quasi-public places. For example, the proportion of local councils in Australia that have or plan to have open street CCTV increased from one in ten in 2005 to more than two thirds in 2015.[76]

[2.44] In addition, surveillance technologies exist within a wider framework of enhanced capabilities for storing, analysing, combining and sharing data. People are at greater risk of exposure where greater volumes of data about them are being generated and accessed than was possible before.

[2.45] The increase in sophistication and accessibility of surveillance technologies also increases the tension between the perceived benefits of those technologies to consumers and the value to third parties of the information generated by consumers' use of those technologies.

[2.46] These features combine to increase the scope for surveillance technologies to be used in ways that challenge community expectations and understandings of privacy. In particular, they may impact on what is considered a reasonable expectation of privacy.[77]

[2.47] Particular privacy risks include:[78]

- Intrusiveness—where surveillance is of activities or in locations that carry a high expectation of privacy, or where the type of surveillance is considered disproportionate to its purpose.
- Intensity—where individuals are subject to surveillance for longer periods, more closely and in 'higher resolution'.
- Extensiveness—where, due to increased accessibility of surveillance technologies, surveillance occurs more often and in more places.

---

74 Deloitte, *Mobile Consumer Survey 2017* (2017) 4.

75 J Pearlman, 'Rise of the drone poses regulation headache for Australia', *The Straits Times* (online), 26 January 2018. The precise number is not known because drones do not need to be registered to be flown recreationally. CASA has received more than 6000 notifications of intent to conduct commercial drone operations in Australia: CASA, *Drone Fast Facts* (2017) <https://consultation.casa.gov.au/regulatory-program/dp1708os/>.

76 S Hulme, A Morgan and R Brown, 'CCTV use by local government: Findings from a national survey' (Research in Practice No 40, Australian Institute of Criminology, May 2015) 2–3. Queensland had the highest proportion, with 67% of all Queensland councils having open street CCTV in 2015. See also [2.36] above as to the potential use of CCTV cameras with audio recording capability.

77 See, eg, M Paterson, 'Regulating Surveillance: Suggestions for a Possible Way Forward' (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 193, in which it is suggested that 'reasonable expectations of privacy' is arguably no longer an appropriate test due to technological advancements.

78 See, eg, Office of the Victorian Information Commissioner (formerly Commissioner for Privacy and Data Protection), *Guidelines to Surveillance and Privacy in the Victorian Public Sector* (May 2017) 10; Clarke, above n 22, [3.2]. See also, eg, NSWLRC Report No 98 (2001) [2.23]; ACT Review (2016) [6.30]; ALRC Report No 123 (2014) [6.15]; VLRC Information Paper (2001) [1.9]; VLRC Report No 18 (2010) [4.32].

- Lack of transparency and consent—where individuals are not made aware that they are under surveillance, are not able to provide meaningful consent, or do not understand how their information will be used.
- Over-collection—where surveillance generates more information than is necessary for its purpose, such as inadvertently capturing information about bystanders.
- Function creep—where information collected for one purpose is later used for another purpose which may not have initially been anticipated.
- Inaccuracy—where information collected from surveillance is used to draw conclusions about a person or their behaviour that may be incorrect or misleading.

[2.48] A related concern is data insecurity, where information that is being collected or stored is vulnerable to unauthorised disclosure.[79]

[2.49] It has been observed that perceived privacy risks, even if not realised, may undermine the public confidence that is necessary for the successful adoption of new technologies.[80]

[2.50] The importance of trust, and of transparency and accountability, is widely acknowledged in privacy and surveillance contexts.[81] For example:[82]

> Technological change is accompanied by trust as expectation: the expectation that the state has a duty of care and that whatever government is in office will exercise its powers and deliver the means of protecting us from new dangers. In relation to privacy and surveillance, levels of trust are vulnerable if government appears unresponsive or is deemed too slow to react to the dangers posed by the use of those technologies.

[2.51] Legislation regulating the use of surveillance devices is one means of protecting against risks to privacy and, in so doing, assisting in maintaining reasonable expectations of privacy within the community, particularly 'as the public becomes increasingly accustomed to being watched'.[83]

---

79 See n 43 above.

80 See, eg, Federal Trade Commission (USA), 'Internet of Things: Privacy and Security in a Connected World' (FTC Staff Report, January 2015) 18.

81 See, eg, Australian Computer Society, 'Data Sharing Frameworks' (Technical White Paper, September 2017) ch 10; The Royal Academy of Engineering, 'Dilemmas of Privacy and Surveillance: Challenges of Technological Change' (Report, March 2007) [8.1]; V Pavone, S Degli-Esposti and E Santiago, 'Key factors affecting public acceptance and acceptability of SOSTs' (Report, D2.4, SurPRISE, 2015) 154–5.

82 The Royal Academy of Engineering, above n 81 [8.1.1].

83 NSWLRC Report No 108 (2005) [4.20].

Community attitudes about privacy and surveillance

[2.52] Community attitudes about privacy and surveillance are complex. Overall, Australian research shows an ongoing community concern for privacy.[84] It has also been observed that 'privacy is increasingly becoming an asset'.[85]

[2.53] For example, the most recent community attitudes survey by the Office of the Australian Information Commissioner (the 'OAIC') showed that 69% of respondents are more concerned about online privacy than they were five years ago, and many have avoided dealing with a private organisation due to privacy concerns (58%). However, only 37% regularly read privacy policies, 48% clear their online browsing history and 48% adjust their privacy settings.[86]

[2.54] The same survey showed that many people are concerned about the possibility of becoming the victim of identity fraud and theft (69%), and about the use of biometric data in a variety of day to day situations including in the use of technology such as smartphones or fitness trackers (55%).[87]

[2.55] Other research has found that, with the exception of access to data by law enforcement and security agencies, there is a general level of concern about the collection of telecommunications data. However, people are more evenly divided in their views of government programs that track their use of public services and benefits.[88]

[2.56] Understandings of and attitudes to privacy are culturally dependent, but research in other jurisdictions also shows generally high levels of community concern about privacy and surveillance.[89]

[2.57] For example, the most recent national survey conducted for the Privacy Commissioner of New Zealand found that 55% of respondents are more concerned with their individual privacy than they were in the last few years. Of particular interest, the survey found that over 62% of respondents are concerned with the use of drones in residential areas, and 36% are concerned about the use of CCTV by individuals.[90]

---

84 See, eg, OAIC, 'Australian Community Attitudes to Privacy Survey 2017' (Report, May 2017); G Goggin et al, 'Digital Rights in Australia' (Report, University of Sydney, November 2017); M Richardson et al, 'Towards responsive regulation of the Internet of Things: Australian perspectives' (2017) 6(1) *Internet Policy Review* 1.

85 Evidence to Standing Committee on Law and Justice, Parliament of New South Wales, Sydney, 30 October 2015, 2 (E Coombs, NSW Privacy Commissioner, Information and Privacy Commission).

86 See OAIC, above n 84, 17–19, Figs 17, 18. The OAIC undertakes regular community attitudes surveys (to date, in 2001, 2004, 2007, 2013 and 2017). The surveys primarily focus on information privacy.

87 Ibid 21, 33–4, figs 20, 36. At the same time, concern about the use of biometric data has decreased for access to licensed premises (from 71% in 2013 to 58% in 2017) and access to places of work or study (from 55% in 2013 to 46% in 2017).

88 See, eg, Goggin et al, above n 84, ch 4.

89 See [2.57]–[2.58] below. See also, eg, Pew Research Centre, 'Americans' Attitudes About Privacy, Security and Surveillance' (Report, 20 May 2015) 4.

90 UMR Research, 'Privacy Concerns and Sharing Data' (Report, 2018) 5, 8, 10, 16. Privacy surveys are regularly undertaken for the Privacy Commissioner (to date, in 2001, 2006, 2008, 2010, 2012, 2014, 2016 and 2018).

[2.58] Research in Europe, including the United Kingdom, has found that many people are concerned about the privacy impacts of surveillance technologies, but that their level of discomfort varies depending on the nature of the technology and its perceived intrusiveness. For instance, people are more uncomfortable with mass data surveillance by 'deep packet inspection' (66%) than with targeted surveillance by 'smartphone location tracking' (45%) or with mass surveillance by 'smart CCTV' (39%). Specific concerns about these technologies include future developments in their use, their ability to reveal sensitive personal information such as locational information, and their capacity to lead to misinterpretations of behaviour.[91]

[2.59] It is sometimes observed that there is a gap between people's beliefs about the importance of privacy and the steps they take (or do not take) to protect their privacy, typically in online environments.[92]

[2.60] However, decision-making about privacy is complex.[93] In one study, for example, 67% of respondents said they actively protect their online privacy, but only 38% said they 'feel in control' of their privacy.[94] Although a person might want to protect their privacy, they may also want to use services that necessitate some sharing of their personal information. Further, voluntary disclosure of personal information does not necessarily mean that an individual has given up their interest in what happens to that information or their interest in other aspects of their privacy.[95]

---

91 S Straub, 'Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe—Citizen Summits on Privacy, Security and Surveillance' (Synthesis Report, D6.10, SurPRISE, 2015) [4.3]–[4.4]. The study focused on surveillance used for security purposes.

'Deep-packet inspection' involves opening and analysing messages as they travel on a network; 'smartphone location tracking' analyses location data from a mobile phone to glean information about the location and movements of the phone user over a period of time; 'smart CCTV' involves digital cameras, linked together in a system, that have the potential to recognise people's faces, analyse their behaviour and detect objects: Pavone, Degli-Esposti and Santiago, above n 81, [6.1.1].

92 This has been referred to as the 'privacy paradox', and remains a field of ongoing research: see generally S Barth and MDT de Jong, 'The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behaviour—A systematic literature review' (2017) 34(7) *Telematics and Informatics* 1038.

93 Explanations for the 'privacy paradox' include user trust, lack of risk awareness, risk-benefit analysis, and privacy cynicism: see, eg, CP Hoffmann, C Lutz and G Ranzini, 'Privacy cynicism: A new approach to the privacy paradox' (2016) 10(4) *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, article 7; Francis and Francis, above n 16, 46–8.

Some studies have contradicted the paradox. For example, a study of Swiss internet users found that 'people who worry more about the protection of personal data … apply more measures to protect themselves': C Lutz and P Strathoff, 'Privacy Concerns and Online Behaviour—Not so Paradoxical After All? Viewing the Privacy Paradox through different theoretical lenses' in S Brändli, R Schister and A Tamo (eds), *Changing multi-national companies and institutions—Challenges for economy, law, and society* (2014) 81, 91.

94 Goggin et al, above n 84, 1, [3.2.2]. A significant proportion (25%) do not feel they can control their online privacy.

95 See, eg, K Burkhardt, 'The privacy paradox is a privacy dilemma' on *Internet Citizen* (24 August 2018) <https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/>; NSW Privacy Commissioner, Dr E Coombs, 'Privacy and Technology' (Speech delivered at the National Media, Privacy & Entertainment Conference, 13 June 2013) as to the 'myth [that] privacy is dead'.

Surveillance devices legislation

[2.61] In each Australian jurisdiction, legislation regulates the use of particular categories of surveillance devices and the communication or publication of information resulting from their use ('surveillance devices legislation').[96]

Queensland: *Invasion of Privacy Act 1971*

[2.62] In Queensland, the *Invasion of Privacy Act 1971* regulates listening devices. Section 4 of the Act defines 'listening device' to mean:

> any instrument, apparatus, equipment or device capable of being used to overhear, record, monitor or listen to a private conversation simultaneously with its taking place.

[2.63] Relevantly, a reference to a 'listening device':[97]

> does not include a reference to a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and to permit the person only to hear sounds ordinarily audible to the human ear.

[2.64] Listening devices are regulated only to the extent that they are used in relation to private conversations. Section 4 of the Act defines 'private conversation' to mean:

> any words spoken by one person to another person in circumstances that indicate that those persons desire the words to be heard or listened to only by themselves or that indicate that either of those persons desires the words to be heard or listened to only by themselves and by some other person, but does not include words spoken by one person to another person in circumstances in which either of those persons ought reasonably to expect the words may be overheard, recorded, monitored or listened to by some other person, not being a person who has the consent, express or implied, of either of those persons to do so.

[2.65] It is an offence for a person to use a listening device to overhear, record, monitor or listen to a private conversation unless that person is a party to the conversation (the 'use prohibition').[98] Use by a party without the consent of the other parties—referred to as 'participant monitoring'—is therefore permitted.[99]

[2.66] A reference to a 'party' is a reference to:[100]

---

96 See the comparative table of Australian legislation in Appendix B.

97 *Invasion of Privacy Act 1971* (Qld) s 42(1).

98 *Invasion of Privacy Act 1971* (Qld) s 43(1), (2)(a) (maximum penalty 40 penalty units ($5222) or two years imprisonment). Additionally, the offence does not apply to 'the unintentional hearing of a private conversation by means of a telephone', or in a variety of situations relating to use by law enforcement or particular government entities: s 43(2)(b)–(e).

99 See also [2.79] below.

100 *Invasion of Privacy Act 1971* (Qld) s 42(2). In other jurisdictions, a person who is speaking or spoken to during the course of a conversation is sometimes referred to as a 'principal party', and another person who is present with consent is referred to as a 'party': see [2.77] below. Each of those terms is used where relevant in this paper.

> a person by or to whom words are spoken in the course of a private conversation; and
>
> a person who, with the consent, express or implied, of any of the persons by or to whom words are spoken in the course of a private conversation, overhears, records, monitors or listens to those words.

[2.67] There are also prohibitions on communicating or publishing information (the 'communication or publication prohibitions'):

- a party who uses a listening device is prohibited from communicating or publishing any record of the conversation made, directly or indirectly, by that use of the listening device;[101] and
- a person is prohibited from communicating or publishing a private conversation that has come to that person's knowledge as a direct or indirect result of the unlawful use of a listening device.[102]

[2.68] There are exceptions to each of these prohibitions, including if the communication is with the consent of a party to the conversation.[103]

[2.69] The *Invasion of Privacy Act 1971* also makes provision for other matters, including that:[104]

- where a private conversation has come to a person's knowledge as a direct or indirect result of the unlawful use of a listening device, that person may not ordinarily give evidence of the conversation in civil or criminal proceedings, although there are exceptions;[105] and
- it is an offence to advertise a listening device of a prescribed class or description.[106]

Other jurisdictions

[2.70] Like Queensland, the surveillance devices legislation in the Australian Capital Territory and Tasmania regulates the use of listening devices in relation to private conversations.[107]

[2.71] In contrast, the surveillance devices legislation in New South Wales, the Northern Territory, South Australia, Victoria and Western Australia regulates

---

101 *Invasion of Privacy Act 1971* (Qld) s 45(1) (maximum penalty 40 penalty units ($5222) or two years imprisonment). A party is also prohibited from communicating a statement prepared from a record of the conversation.

102 *Invasion of Privacy Act 1971* (Qld) s 44(1) (maximum penalty 40 penalty units ($5222) or two years imprisonment).

103 See *Invasion of Privacy Act 1971* (Qld) ss 44(2), 45(2).

104 See also *Invasion of Privacy Act 1971* (Qld) s 48A (Unlawful entry of dwelling houses), discussed at [2.132] below.

105 *Invasion of Privacy Act 1971* (Qld) s 46, discussed at [3.207] ff below.

106 *Invasion of Privacy Act 1971* (Qld) s 48. No devices have been prescribed.

107 *Listening Devices Act 1992* (ACT); *Listening Devices Act 1991* (Tas).

'surveillance devices'. In those jurisdictions, surveillance devices legislation initially regulated the use of listening devices only but was later extended to cover additional categories of surveillance device.[108]

[2.72] A 'surveillance device' is defined to mean a listening device, optical surveillance device, tracking device and, except in Western Australia, data surveillance device.[109] 'Listening device' is defined in similar terms to the legislation in Queensland.[110] The other categories of surveillance device are defined as follows:[111]

- *Optical surveillance device*—any instrument, apparatus, equipment or device that can be used to monitor, record visually or observe an activity, excluding spectacles, contact lenses or a similar device used by a person to overcome a vision impairment. In South Australia, the term is more specifically defined to also include observing or recording visually a person, place or activity and to also exclude telescopes, binoculars or other similar devices.
- *Tracking device*—any instrument, apparatus, equipment or device (or, in New South Wales, the Northern Territory and Victoria, an electronic device) that can be used to determine or monitor the geographical location of a person or an object (or, in Victoria, the 'primary purpose' of which is to determine the geographical location of a person or an object).
- *Data surveillance device*—any instrument, apparatus, equipment or device (and, in New South Wales and South Australia, a program) that can be used to monitor or record the input of information into or output of information from a computer (or the information that is being put onto or retrieved from a computer).[112] This does not include an optical surveillance device. In South

---

108 See the *Surveillance Devices Act 2007* (NSW) which replaced the *Listening Devices Act 1984* (NSW); the *Surveillance Devices Act* (NT) of 2007 which replaced an earlier Act of the same name of 2000, which in turn replaced the *Listening Devices Act* (NT) of 1990; the *Surveillance Devices Act 2016* (SA) which replaced the *Listening and Surveillance Devices Act 1972* (SA) as amended by the *Listening Devices (Miscellaneous) Amendment Act 2001* (SA); the *Surveillance Devices Act 1999* (Vic) which replaced the *Listening Devices Act 1969* (Vic); and the *Surveillance Devices Act 1998* (WA) which replaced the *Listening Devices Act 1978* (WA).

109 *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; *Surveillance Devices Act 2016* (SA) s 3(1); *Surveillance Devices Act 1999* (Vic) s 3(1); *Surveillance Devices Act 1998* (WA) s 3(1).

110 See [2.62]–[2.63] above. None of the other jurisdictions, except Tasmania, expressly provide as part of the definition that a listening device is capable of being used 'simultaneously' with the conversation taking place. Tasmania does not exclude a hearing aid or similar device. See the references in n 111 below.

111 *Surveillance Devices Act 2007* (NSW) s 4(1) (definitions of 'device', 'listening device', 'optical surveillance device', 'tracking device' and 'data surveillance device'); *Surveillance Devices Act* (NT) s 4 (definitions of 'device', 'listening device', 'optical surveillance device', 'tracking device' and 'data surveillance device'); *Surveillance Devices Act 2016* (SA) s 3(1) (definitions of 'listening device', 'optical surveillance device', 'tracking device' and 'data surveillance device'); *Surveillance Devices Act 1999* (Vic) s 3(1) (definitions of 'device', 'listening device', 'optical surveillance device', 'tracking device' and 'data surveillance device'); *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of 'listening device', 'optical surveillance device' and 'tracking device'). See also *Listening Devices Act 1992* (ACT) s 2, Dictionary (definitions of 'listening device' and 'hearing aid'); *Listening Devices Act 1991* (Tas) s 3(1) (definition of 'listening device').

112 In New South Wales, the Northern Territory and Victoria, 'computer' is defined to mean any electronic device for storing or processing (and, in New South Wales, for transferring) information.

Australia, it is also defined as a device that can access or track the input or output of that information and associated equipment.[113]

[2.73] The legislation in New South Wales, the Northern Territory, South Australia and Victoria also defines a surveillance device to mean a combination of any two or more of those devices, and enables other kinds of devices to be prescribed by regulation.[114]

[2.74] The regulation of each category of surveillance device is subject to various limitations. In particular:

- a *listening device*—is regulated in each jurisdiction only to the extent that it is used in relation to a 'private conversation' (similar to Queensland).
- an *optical surveillance device*—is regulated:
  - only in relation to a 'private activity' (in the Northern Territory, South Australia, Victoria and Western Australia), which does not include an activity carried on outside a building (in Victoria);[115]
  - in New South Wales and South Australia, only where the use of the device is on or in premises, a vehicle or other thing and (in New South Wales) only if it involves entry on to or into the premises or vehicle, or interference with the vehicle or other object, without consent.[116]
- a *tracking device*—is regulated in Victoria only if the 'primary purpose' of the device is to determine the geographical location of a person or an object.[117]
- a *data surveillance device*—is regulated:
  - in the Northern Territory and Victoria, only in relation to law enforcement officers;[118]

---

113 'Associated equipment' is defined to mean equipment or things used for, or in connection with, the operation of the surveillance device: *Surveillance Devices Act 2016* (SA) s 3(1).

114 See n 109 above. No other kind of device has been prescribed by regulation in those jurisdictions.

115 *Surveillance Devices Act* (NT) s 12(1); *Surveillance Devices Act 2016* (SA) s 5(1)–(3); *Surveillance Devices Act 1999* (Vic) s 7(1); *Surveillance Devices Act 1998* (WA) s 6(1). See also n 123 below.

116 See *Surveillance Devices Act 2007* (NSW) ss 4(1), 8(1); *Surveillance Devices Act 2016* (SA) ss 3(1), 5(1)–(3). 'Premises' is defined to include land, a building, part of a building and any place whether built on or not, whether in or outside the jurisdiction.

117 *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'tracking device'). Consequently, in Victoria, a device that is capable of tracking, but is not primarily used for that purpose (such as a smartphone with GPS capability), is not a tracking device covered by the Act: VLRC, Report No 18 (2010) [6.29] ff. The VLRC recommended that the 'primary purpose' requirement in the definition of tracking device should be removed and the definition be made consistent with the other jurisdictions 'that are concerned with the capacity of the device rather than its primary purpose'. However, it also recommended that the legislation should include exceptions to permit legitimate uses of tracking devices.

118 *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9.

- in New South Wales, only where the use involves entry onto or into the premises without the express or implied consent of the owner or occupier of the premises, or interference with the computer or a computer network on the premises without the express or implied consent of the person having lawful possession or lawful control of the computer or computer network;[119]

- in South Australia, only where a person installs, uses or maintains a data surveillance device to access, track, monitor or record the input of information into, the output of information from, or information stored in, a computer without the express or implied consent of the owner, or person with lawful control or management, of the computer.[120]

[2.75] The regulation of a listening device and, except in New South Wales, an optical surveillance device is linked to the concept of a 'private conversation' or a 'private activity'. Consistently with the legislation in Queensland,[121] these concepts are defined as follows:[122]

- *private conversation*—a conversation between parties (or words spoken by one person to others) carried on in circumstances that may reasonably be taken to indicate that one or all of the parties want the words to be heard or listened to only by themselves (or only by themselves and some other person); and

- *private activity*—an activity carried on in circumstances that may reasonably be taken to indicate that one or all of the parties do not want the activity to be observed, except by themselves.[123]

[2.76] Except in the Australian Capital Territory and Tasmania, this does not include a conversation or activity carried on in circumstances where one or all of the parties ought reasonably to expect that the conversation might be overheard or the activity observed.[124]

---

119 *Surveillance Devices Act 2007* (NSW) s 10(1). For the meaning of premises see n 116 above.

120 *Surveillance Devices Act 2016* (SA) s 8(1).

121 See [2.64] above.

122 *Listening Devices Act 1992* (ACT) s 2 Dictionary; *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; *Surveillance Devices Act 2016* (SA) s 3(1); *Listening Devices Act 1991* (Tas) s 3(1); *Surveillance Devices Act 1999* (Vic) s 3(1); *Surveillance Devices Act 1998* (WA) s 3(1). The legislation in the Australian Capital Territory, New South Wales and Tasmania defines 'private conversation' only.

123 In South Australia, a private activity does not include an activity carried on in a public place, or carried on in premises or a vehicle if it can be readily observed from a public place. A 'public place' includes a place where free access is permitted to the public; a place where the public are permitted on payment of money; or a road, street, footway, court, alley or thoroughfare that the public are allowed to use even though it is on private property: *Surveillance Devices Act 2016* (SA) s 3(1) (definition of 'public place'). As to the definition of 'premises', see n 116 above.

In Victoria, a private activity does not include an activity carried on outside a building. The VLRC noted that, consequently, there is no protection against highly intrusive visual surveillance in outdoor places, such as beaches or backyards: VLRC Report No 18 (2010) [6.9]–[6.10].

124 See also ACT Review (2016) [6.7], in which it was recommended that surveillance devices legislation should make it clear that a private conversation or activity is limited where the parties can reasonably expect to be overheard or observed by others. It was explained that:

[2.77] A 'party' to a private conversation is defined:[125]

- in each jurisdiction, to mean a person by or to whom words are spoken in the course of the conversation (referred to as a 'principal party' in the Australian Capital Territory, New South Wales, South Australia, Tasmania and Western Australia);
- in the Australian Capital Territory, New South Wales, Tasmania and Western Australia (like Queensland) to also include a person who listens to, monitors or records a conversation with the express or implied consent of any of the principal parties to the conversation.

[2.78] A 'party' to a private activity is defined as a person who takes part in the activity.[126] However, in Western Australia a person who takes part in the activity is a 'principal party', and a 'party' is a person who observes or records the activity with the express or implied consent of a principal party.[127]

[2.79] In Victoria and the Northern Territory (similarly to Queensland) a party to a private conversation or activity is permitted to use a listening device or optical surveillance device to record the conversation or activity, without the knowledge or consent of the other participants.[128] This is commonly referred to as 'participant monitoring'.[129] In contrast, the majority of jurisdictions prohibit participant monitoring, and instead include exceptions that set out the circumstances in which a surveillance device may be used by a party.[130]

[2.80] The surveillance devices legislation in each jurisdiction also includes communication or publication prohibitions. Like Queensland, jurisdictions where the legislation is limited to a listening device include separate offences that apply to a party and to another person.[131] Other jurisdictions include more general offence

---

This reflects an approach that, although a broad range of devices might come within the definition of a listening, optical, tracking or data surveillance device (given that any device only has to be capable of those functions), their use in public places will generally not give rise to privacy concerns.

125 *Listening Devices Act 1992* (ACT) s 2 Dictionary (definitions of 'consent', 'party' and 'principal party'); *Surveillance Devices Act 2007* (NSW) s 4(1) (definitions of 'party' and 'principal party'); *Surveillance Devices Act* (NT) s 4 (definition of 'party'); *Surveillance Devices Act 2016* (SA) s 3(1) (definition of 'principal party'); *Listening Devices Act 1991* (Tas) s 3(1) (definitions of 'party' and 'principal party'); *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'party'); *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of 'party' and 'principal party').

126 *Surveillance Devices Act* (NT) s 4 (definition of 'party'); *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of 'party'). See also *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of 'party') which applies in relation to an 'activity'.

127 *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of 'party' and 'principal party').

128 *Surveillance Devices Act* (NT) ss 11(1)(a), 12(1)(a); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1). The provisions in New South Wales about an optical surveillance device, which do not require the consent of those being recorded, may also have a similar effect: *Surveillance Devices Act 2007* (NSW) s 8(1).

129 See ACT Review (2016) [6.9]; VLRC Report No 18 (2010) [6.54]; VLRC Consultation Paper No 7 (2009) [5.21], [6.132]; ALRC Report No 123 (2014) [14.48].

130 *Listening Devices Act 1992* (ACT) s 4(1)(b), (2)–(4); *Surveillance Devices Act 2007* (NSW) s 7(1)(b), (2)–(3); *Surveillance Devices Act 2016* (SA) ss 4(1)(b), (2)–(3), 5; *Listening Devices Act 1991* (Tas) s 5(1)(b), (2)–(7); *Surveillance Devices Act 1998* (WA) ss 5(1)(b), (2)–(3), 6(1)(b), (2)–(3). In New South Wales, optical surveillance devices are treated differently: see n 128 above.

131 *Listening Devices Act 1992* (ACT) ss 5, 6; *Listening Devices Act 1991* (Tas) ss 9, 10. See also [2.67] above.

provisions that apply to any user of a relevant surveillance device.[132] The provisions vary in their application to information that was obtained through the lawful or unlawful use of a device.

[2.81] In each jurisdiction, the surveillance devices legislation includes exceptions that permit the use of a surveillance device, or the communication or publication of information obtained from the use of a surveillance device, in particular circumstances. This may, for example, include use, communication or publication with the consent of the parties to the private conversation or activity.

Surveillance and law enforcement in Queensland

[2.82] In Queensland, chapter 13 of the *Police Powers and Responsibilities Act 2000* (the 'PPRA') separately regulates the use of a listening device, optical surveillance device, data surveillance device or tracking device by law enforcement officers.[133] The *Surveillance Devices Act 2004* (Cth) regulates the use of those devices by federal law enforcement officers.

[2.83] Both Acts establish procedures for law enforcement officers to obtain warrants and authorisations to use a surveillance device in criminal investigations and other situations. They also restrict the use, communication or publication of information obtained through use of a surveillance device. The PPRA provides for the recognition of warrants and authorisations issued in other Australian jurisdictions.[134]

[2.84] The *Surveillance Devices Act 2004* (Cth) and chapter 13 of the PPRA are based on model legislation which was developed to achieve uniform regulation of the use of surveillance devices by law enforcement agencies in Australian jurisdictions and provide for the mutual recognition of warrants, in order to facilitate cross-border investigations.[135] The model legislation was intentionally similar to existing state and territory legislation because the intended outcome was to achieve harmonisation and facilitate cross-border operations.[136]

---

132 *Surveillance Devices Act 2007* (NSW) ss 11, 14; *Surveillance Devices Act* (NT) s 15; *Surveillance Devices Act 2016* (SA) pt 2 div 2; *Surveillance Devices Act 1999* (Vic) s 11; *Surveillance Devices Act 1998* (WA) s 9.

133 See also the *Crime and Corruption Act 2001* (Qld) ch 3 pt 6 which regulates the use of surveillance devices by authorised officers of the Crime and Corruption Commission. This Act also provides a process for obtaining a warrant to use a surveillance device in particular circumstances.

The terms of reference exclude the existing law regulating the use of surveillance devices for State law enforcement purposes from the review: see terms of reference, para E.

134 See generally *Police Powers and Responsibilities Act 2005* (Qld) s 321; *Surveillance Devices Act 2004* (Cth) s 3.

135 See Joint Working Group Report (2003) 345; Explanatory Note, Cross-Border Law Enforcement Legislation Amendment Bill 2005 (Qld) 1–2; Explanatory Memorandum, Surveillance Devices Bill 2004 (Cth) 1.

136 Joint Working Group Report (2003) 347.

[2.85] The model legislation was implemented in Queensland by the insertion of chapter 13 of the PPRA.[137] Other jurisdictions, such as New South Wales, have enacted a single Act, based on the model legislation, which regulates the use of a surveillance device by both individuals and law enforcement officers.[138]

137 See *Cross-Border Law Enforcement Legislation Amendment Act 2005* (Qld) s 28.

138 See, eg, *Surveillance Devices Act 2007* (NSW); Explanatory Note, Surveillance Devices Bill 2007 (NSW) 1. See also Surveillance Devices Amendment (Statutory Review) Bill 2018 (NSW).

Other laws relevant to surveillance and privacy

[2.86] In Queensland, surveillance and privacy are regulated under both State and Commonwealth legislation. The common law may also be relevant. Some key aspects of the law are discussed below.

Telecommunications

[2.87] Under the Australian Constitution, the Commonwealth has the power to make laws with respect to 'postal, telegraphic, telephonic and other like services'.[139] The Commonwealth has enacted the *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Telecommunications Act 1997* (Cth). It has been observed that both Acts recognise and protect the privacy of individuals who communicate through the Australian telecommunications network.[140]

[2.88] The High Court has determined that the *Telecommunications (Interception and Access) Act 1979* (Cth) exclusively regulates the interception of telephone conversations,[141] and it is considered 'highly likely' that it also exclusively regulates the interception of other communications using a telecommunications network, for example short message services (commonly referred to as 'SMS' or 'text messages') and emails.[142]

Interception of telecommunications

[2.89] Under the *Telecommunications (Interception and Access) Act 1979* (Cth), it is generally an offence for a person to intercept a communication passing over a telecommunications system without the knowledge of the person making the communication. It is also an offence to authorise, suffer or permit another person to intercept such a communication, or to do any act or thing that will enable him or her or another person to intercept such a communication.[143]

[2.90] The offence applies to a communication on a landline or a mobile phone, and communications that are in transit over the internet and through internet service provider facilities.[144] Some common examples of a 'communication' are a telephone

---

139 *Australian Constitution* s 51(v).

140 *Smith v The Queen* (1991) 52 A Crim R 447, 449; L-J Vanhear, 'Hello … Is anybody there? … The law on recording private conversations' (2014) 11(10) *Privacy Law Bulletin* 193, 193; S Alderson, 'Interception of and access to communications', *Communications Law and Policy in Australia* (2011) [610,700]. The Australian Government explains that the *Telecommunication (Interception and Access) Act 1979* (Cth) 'protects the privacy of Australians by prohibiting interception of communications and access to stored communications': Department of Home Affairs, Australian Government, *Telecommunications interception and surveillance* (11 November 2018) <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/data-retention-and-interception/telecommunications-interception-and-surveillance>.

141 *Miller v Miller* (1978) 141 CLR 269, 276.

142 See VLRC Report No 18 (2010) [1.22].

143 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 6(1), 7(1), 105(1)–(2) (maximum penalty two years imprisonment).

144 See Vanhear, above n 140, 194; Electronic Frontiers Australia, *Telecommunications (Interception and Access) Act 1979 (TIA)* (2018) <https://www.efa.org.au/privacy/tia-new/>.

The VLRC also stated that '[m]ost practices involving the use of computer software to spy on the activities of others via the internet involve telecommunications interceptions': VLRC Report No 18 (2010) [1.23].

conversation, a text message or an email.[145] Communications solely by means of radiocommunication, such as bluetooth or walkie-talkie communications, are not included.[146]

[2.91] A communication is intercepted if it is listened to or recorded, by any means, while it is being transmitted between the persons communicating, without the knowledge of the person who is making the communication.[147] A communication will be in transmission from the time that it is sent or transmitted by the sender, until the time that it becomes accessible to the intended recipient; for example, the period of time between an SMS being sent and being delivered to the recipient's telephone provider.[148]

[2.92] Effectively, the prohibition against interception is limited to 'live' or 'real-time' communications.[149] Once a communication is no longer being transmitted, a person is not prohibited by the *Telecommunications (Interception and Access) Act 1979* (Cth) from recording the conversation.[150] One commentator explains that:[151]

> recordings made by an external device after the sound of a speaker's voice has left the telecommunications system, such as through the use of an external microphone or tape recording, will technically not constitute an 'interception' for the purposes of the [Act]. (notes omitted)

The offence applies in relation to a 'telecommunications system'. This is defined to mean a telecommunications network that is within or partly within Australia and equipment, a line or other facility that is connected to such a network and is within Australia. A 'telecommunications network' is defined to mean a system (or series of systems) for carrying communications by means of electromagnetic energy, but not a system (or series of systems) for carrying communications solely by means of radiocommunication: *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(1).

145 A 'communication' is defined to include all or part of a conversation or a message and may be in any form including speech, music or other sounds, data, text, visual images or signals: *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(1).

146 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(1) (definitions of 'telecommunication network' and 'telecommunications system'). See also VLRC Report No 18 (2010) [1.22].

147 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6(1). Specifically, the Act states that 'interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'. Knowledge does not necessarily require consent, but the person must be aware of the interception: Vanhear, above n 140, 194.

148 Relevantly, the *Telecommunications (Interception and Access) Act 1979* (Cth) applies to the interception of a communication 'passing over a telecommunications system': ss 6(1), 7(1). The Act states that 'a communication is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication': s 5F. A communication is 'accessible' if it has been received by or delivered to the telecommunications service provided to the intended recipient, or is under the control of the intended recipient (although this is not exhaustive): s 5H. The 'intended recipient' is the individual or person to whom the communication is addressed, or otherwise to the person who has control over the telecommunications service to which the communication is sent: s 5G.

149 See Electronic Frontiers Australia, *Telecommunications (Interception and Access) Act 1979 (TIA)* (2018) <https://www.efa.org.au/privacy/tia-new/>.

150 However, other legislation relevant to the recording of conversations (such as state and territory legislation about the use of a listening device) will continue to apply.

151 Vanhear, above n 140, 194, citing *Telecommunications (Interception and Access) Act 1979* (Cth) s 7(1), *R v Evans* (1999) 152 FLR 352 and *R v Oliver* (1984) 57 ALR 543, 548. See also *R v Migliorini* (1981) 4 A Crim R 458; *R v Curran* [1982] 2 VR 133; Alderson, above n 140, [610,800]; VLRC Report No 18 (2010) [1.22]; NSWLRC Report No 108 (2005) [2.4].

[2.93] It is also an offence for a person who obtained information by lawfully or unlawfully intercepting a communication to communicate that information to another person, make use of or make a record of that information, or give evidence in a proceeding about that information.[152]

Accessing stored communications

[2.94] Stored communications, being communications that are not in transit and that have been held by a 'carrier' of communications services, are also protected.[153] Common examples of stored communications are emails, text messages and voice mail messages that are not in transit.[154]

[2.95] It is an offence for a person to access a stored communication, authorise, suffer or permit another person to access a stored communication, or do any act or thing that will enable them or another person to access a stored communication.[155] The offence applies if the access (or other act or thing) occurs without the knowledge of either the intended recipient or the person who sent the stored communication.[156]

[2.96] The 'accessing' of a stored communication is defined as 'listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication'.[157] A person is not prohibited (by this provision) from accessing a communication, that is no longer in transit, from the intended recipient or from a device that is in the intended recipient's possession.[158]

---

152 *Telecommunications (Interception and Access) Act 1979* (Cth) s 63(1). See also s 5A as to the communication of a record obtained by interception, which is taken to communicate as much of the information obtained by interception as can be derived from the record.

153 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1). Specifically, a 'stored communication' is defined as a communication that is not passing over a telecommunications system, and is held on equipment operated by and in the possession of a carrier, and cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier: *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(1). See n 145 above, as to the definition of 'communication'.

A 'carrier' is defined as a carrier or carriage service provider under the *Telecommunications Act 1997* (Cth): *Telecommunications (Interception and Access) Act 1979* (Cth) s 5(1). Relevantly, a 'carrier' is a person who is licenced as the owner of a network unit that is used to supply carriage services to the public. A 'carriage service provider' is a person who supplies or proposes to supply a carriage service to the public using a network unit. A 'carriage service' is 'a service for carrying communications by means of guided and/or unguided electromagnetic energy'. Broadly, the term 'network unit' refers to connections between different places to carry communications or supply carriage services: see *Telecommunications Act 1997* (Cth) ss 5, 7 (definitions of 'carriage service', 'carriage service provider', 'carrier' and 'carrier licence', 'line' and 'network unit'), 41, pt 2 div 2, 56, 87.

154 Electronic Frontiers Australia, *Telecommunications (Interception and Access) Act 1979 (TIA)* (2018) <https://www.efa.org.au/privacy/tia-new/>. A stored communication may not have commenced passing over a telecommunications system, or it may have completed passing over a telecommunications system but be stored on the carrier's equipment.

155 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 108(1)(a) (maximum penalty two years imprisonment or 120 penalty units ($25 200), or both).

156 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1)(b). A person is taken to have knowledge if they are given a written notice of intention to do the act: s 108(1A).

157 *Telecommunications (Interception and Access) Act 1979* (Cth) s 6AA.

158 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1), note. Other legislation might operate to prevent access by such means.

Privacy and telecommunications

[2.97] The *Telecommunications Act 1997* (Cth) contains a specific regime for the protection of communications.[159]

[2.98] Generally, carriage service providers,[160] operators of emergency call services and operators of a public number database (and their respective associates) are required to protect the confidentiality of information or documents that relate to:[161]

- the contents or substance of communications[162] that have been or are being carried[163] by carriers or carriage service providers;
- carriage services supplied or intended to be supplied by carriers or carriage service providers; and
- the affairs[164] or personal particulars (including any unlisted telephone number or any address) of other persons.

[2.99] The use or disclosure of information or documents relating to those matters is generally prohibited, except in limited circumstances, for example, with consent or if authorised under another law.[165]

Privacy

Right to privacy

[2.100] In Queensland, the Human Rights Bill 2018 includes a provision to 'protect and promote human rights' and 'build a culture in the Queensland public sector that respects and promotes human rights'. The Bill requires public entities to act in a way that is compatible with human rights.[166]

[2.101] The Bill proposes a right to 'privacy and reputation', under which individuals have a right not to have their privacy, family, home or correspondence unlawfully or

---

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

160 For definitions of 'carriage service provider' and related terms, see n 153 above. This would include a provider of telephone or internet services.

161 *Telecommunications Act 1997* (Cth) ss 270, 276, 277, 278 (maximum penalty two years imprisonment).

162 The term 'communications' is defined broadly to include communications between persons and persons, persons and things or things and things. Communications may be in the form of speech, music or other sounds, data, text, visual images, signals or another form or combination of forms: *Telecommunications Act 1997* (Cth) s 7.

163 To 'carry' is defined to include 'transmit, switch and receive': *Telecommunications Act 1997* (Cth) s 7.

164 Information or a document about the location of a mobile telephone handset or another mobile communications device is taken to relate to the 'affairs' of the customer responsible for the handset or device: *Telecommunications Act 1997* (Cth) s 275A.

165 *Telecommunications Act 1997* (Cth) pt 13 divs 3–3B. See also Alderson, above n 140, [610,700].

166 Human Rights Bill 2018 (Qld) cll 3(a)–(b), 4(b), pt 3 div 4. The term 'public entity' includes, for example, government entities, the Queensland Police Service and local governments: cl 9. The Bill was introduced into Parliament on 31 October 2018 and was referred to the Legal Affairs and Community Safety Committee for report by 4 February 2019.

arbitrarily interfered with, and not to have their reputation unlawfully attacked.[167] This right may be subject only to reasonable and justifiable limits.[168]

[2.102] The Bill includes a system for dealing with human rights complaints. The Queensland Human Rights Commission is provided with wide powers to resolve complaints, including powers to compel parties to attend conciliation, publish the outcomes of complaints and make public recommendations in relation to complaints.[169]

Information privacy

[2.103] Information privacy in connection with government agencies and some other entities is regulated by separate State and Commonwealth legislation, although the two schemes have a number of similarities. There is similar information privacy legislation in other Australian states and territories.[170]

Queensland

[2.104] In Queensland, the *Information Privacy Act 2009* (the 'IP Act') regulates the way in which Queensland government agencies (for example, Ministers, departments, local governments and public authorities)[171] collect, store, use or disclose personal information.

[2.105] 'Personal information' is defined in the IP Act as:[172]

---

167 Human Rights Bill 2018 (Qld) cll 11, 25. This right is based on art 17 of the ICCPR: see Appendix E.

168 Human Rights Bill 2018 (Qld) cl 13. The Bill provides a non-exhaustive list of factors that may be relevant in determining whether a limit is reasonable and justifiable: cl 13(2).

169 Human Rights Bill 2018 (Qld) pt 4.

170 See, eg, *Information Privacy Act 2014* (ACT); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Act* (NT); *Personal Information Protection Act 2004* (Tas); *Privacy and Data Protection Act 2014* (Vic). There is no specific legislation in South Australia or Western Australia. In South Australia, an administrative instruction requires government agencies to comply with a set of Information Privacy Principles and the Privacy Committee of South Australia has been established to handle complaints. In Western Australia, various confidentiality provisions apply to government agencies and some privacy principles are included in the *Freedom of Information Act 1992* (WA). See generally OAIC, Australian Government, *Other privacy jurisdictions—State and territory privacy* <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions#toc>.

171 Relevantly, an 'agency' is defined to mean a Minister, department, local government or public authority, and includes a body comprised within the agency: s 18(1), (3). However, particular agencies are excluded, including: the Legislative Assembly and members and committees thereof; commissions of inquiry; government owned corporations; and courts and tribunals, and officers or members of a court or tribunal or its registry, in relation to the court's or tribunal's judicial functions: ss 18(2), 19, sch 2.

In certain circumstances, a service provider which has a service arrangement with an agency must also comply with the IPPs in relation to the discharge of its obligations under the arrangement as if it were the entity that is the contracting agency. If the arrangement involves an exchange of personal information, the agency must take all reasonable steps to bind the contracted service provider to the IPPs and NPPs. As a result, the bound contracted service provider assumes privacy obligations as if they were a government agency: ss 34–36, sch 5 (definition of 'bound contracted service provider').

172 *Information Privacy Act 2009* (Qld) s 12. In relation to the similar definition in the *Privacy Act 1988* (Cth), see Explanatory Note, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 61 in which it was stated that:

> information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

[2.106] The IP Act imposes a general obligation on Queensland government agencies to comply with the Information Privacy Principles ('IPPs').[173] Among other things, the IPPs provide that:

- personal information must be collected only for a lawful purpose (IPP 1);
- individuals must be informed about what the information will be used for as soon as practicable, and the information must be relevant, accurate, complete, up-to-date and not unreasonably intrusive (IPPs 2 and 3);
- information must be securely stored and protected from unauthorised access, use, modification, disclosure or any other misuse (IPP 4);
- individuals must be able to find out about the types of information held by an agency and the purposes for which the information is used, and to access documents containing their personal information (IPPs 5 and 6);
- an agency must use only the parts of the personal information that are directly relevant to fulfilling a purpose (IPP 9);
- where personal information has been obtained for a particular purpose, the information must not be used for another purpose (IPP 10); and
- personal information must not be disclosed to a third party (IPP 11).

[2.107] There are a number of exceptions to IPPs 10 and 11, including if:[174]

- the individual the subject of the information has expressly or impliedly agreed to the use or disclosure;
- the use or disclosure is authorised or required under another law; or
- the agency is satisfied on reasonable grounds that the use or disclosure is necessary for law enforcement purposes, or to lessen or prevent a serious

---

> Whether an individual can be identified or is reasonably identifiable depends on context and circumstances. While it may be technically possible for an agency or organisation to identify individuals from information it holds, for example, by linking the information with other information held by it, or another entity, it may be that it is not practically possible. For example, logistics or legislation may prevent such linkage. In these circumstances, individuals are not 'reasonably identifiable'. Whether an individual is reasonably identifiable from certain information requires a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify him or her.

173 *Information Privacy Act 2009* (Qld) s 27. The IPPs are set out in sch 3 of the Act. All agencies, except Queensland Health, must comply with the IPPs. Queensland Health must comply with the National Privacy Principles ('NPPs'), which are set out in sch 4 of the Act.

174 *Information Privacy Act 2009* (Qld) sch 3 IPP 10(1)(a)–(d), 11(1)(b)–(e). If an agency discloses personal information under those exceptions, it must take all reasonable steps to ensure that the entity to which it is disclosed will not use or disclose the information for a purpose other than the purpose for which the information was disclosed: *Information Privacy Act 2009* (Qld) sch 3 IPP 11(3).

threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.

[2.108] There are some exceptions to the general obligation for agencies to comply with the IPPs, particularly for law enforcement agencies (including the Queensland Police Service).[175]

[2.109] If an individual believes that an agency has breached the IPPs in relation to their personal information, they may make a privacy complaint, in the first instance to the agency, or subsequently to the Information Commissioner. If the complaint cannot be satisfactorily resolved, it may be referred to the Queensland Civil and Administrative Tribunal ('QCAT').[176]

[2.110] The Information Commissioner, supported by the Privacy Commissioner, performs various functions under the IP Act, including the management and mediation of privacy complaints and education and training about privacy compliance.[177] The Information Commissioner may issue guidelines to Queensland government agencies, including about how the IP Act should be applied and about privacy best practice.[178]

[2.111] The Information Commissioner has issued guidelines about the use of camera surveillance[179] and the use of drones.[180] Generally, these provide that, where a Queensland government agency captures personal information using camera surveillance or a drone that makes video or audio recordings, the agency must ensure that the collection, storage, use and disclosure of that information complies with the privacy obligations in the IP Act.

Commonwealth

[2.112] Similar to Queensland legislation, the *Privacy Act 1988* (Cth) regulates the way in which certain entities collect or hold personal information.[181]

---

175 See *Information Privacy Act 2009* (Qld) ss 11, 29, sch 5 (definition 'law enforcement agency' para (b)(i)). See also s 28 under which compliance with IPP 8, 9, 10 or 11 is not required in relation to personal information that is related to or connected with personal information of the same individual that has previously been published, or given for the purpose of publication, by the individual.

176 See *Information Privacy Act 2009* (Qld) ch 5.

177 See *Information Privacy Act 2009* (Qld) ch 4; Office of the Information Commissioner (Qld), *Key functions* (2018) <https://www.oic.qld.gov.au/about/our-organisation/key-functions>. See also *Right to Information Act 2009* (Qld) ch 4, under which the role of Information Commissioner is established. The Privacy Commissioner has particular responsibility for matters related to the IP Act: see *Information Privacy Act 2009* (Qld) ch 4 pt 3.

178 *Information Privacy Act 2009* (Qld) s 135(1)(c).

179 Office of the Information Commissioner (Qld), *Guideline: Camera Surveillance and Privacy* (12 July 2018). In the guideline, the term 'camera surveillance' includes any equipment used to observe and record images of individuals such as CCTV, temporary or fixed cameras (such as ANPR cameras), body-worn video cameras and unmanned aerial vehicles. See also Office of the Information Commissioner (Qld), *Guideline: Managing access to digital video recordings* (18 June 2015).

180 Office of the Information Commissioner (Qld), *Guideline: Drones and the Privacy Principles* (16 April 2018). See also Office of the Information Commissioner (Qld), *Top Privacy Tips: Drones*.

181 'Personal information' is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not: *Privacy Act 1988* (Cth) s 6(1).

[2.113] The *Privacy Act 1988* (Cth) applies to 'APP entities', namely a Commonwealth agency (or its contracted service provider), a health service provider, a private sector organisation with an annual turnover of more than $3 million or a business which trades in personal information.[182] An APP entity is required to comply with the Australian Privacy Principles ('APPs') in the Act.[183]

[2.114] Many of the APPs are generally similar to the Queensland IPPs, but there are some differences. For example, the APPs require all APP entities to have a privacy policy and to provide a different level of protection for 'sensitive information'.[184]

[2.115] The *Privacy Act 1988* (Cth) also allows an individual to make a complaint to the Australian Information Commissioner about an act or practice that may be an interference with the privacy of the individual.[185]

[2.116] Under the notifiable data breaches scheme in Part IIIC of the *Privacy Act 1988* (Cth), APP entities also have an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

Criminal offences

[2.117] In Queensland, some serious breaches of privacy are recognised by the criminal law.

Observations or recordings in breach of privacy

[2.118] Section 227A of the Criminal Code contains two separate offences about observing or recording a person in breach of their privacy.[186]

[2.119] It is an offence to observe or visually record another person in a private place or doing a private act, without consent and in circumstances where a reasonable adult would expect to be afforded privacy.[187] A 'private act' means showering or bathing, using a toilet, another activity in which a person is in a state of undress, or intimate sexual activity that is not ordinarily done in public. A 'private

---

See also the Privacy Amendment (Re-Identification Offence) Bill 2016 (Cth), introduced into the Australian Senate on 12 October 2016, which proposes to make it an offence for an entity to re-identify de-identified information published or released by a Commonwealth entity.

182 *Privacy Act 1988* (Cth) ss 6 (definitions of 'agency', 'APP entity' and 'organisation'), 6C–6FB.

183 *Privacy Act 1988* (Cth) ss 14, 15, sch 1.

184 See *Privacy Act 1988* (Cth) sch 1, APP 1 (open and transparent management of personal information), APP 3 (collection of solicited personal information), APP 7 (direct marketing).

185 See *Privacy Act 1988* (Cth) pt V.

186 Criminal Code (Qld) ss 227A(1), (2) (maximum penalty two years imprisonment). The Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 (Qld) proposes to increase the penalty to three years imprisonment: cl 6. The Bill also includes provisions to define consent to mean 'consent freely and voluntarily given by a person with the cognitive capacity to give the consent', make minor changes to the definition of 'genital or anal region', amend the definition of 'state of undress' to include a transgender or intersex person who identifies as female, and allow for the making of rectification orders: cll 4(2), 6(2), 9. See further n 192 below.

187 Criminal Code (Qld) s 227A(1). The Code gives the example of a person who is changing in a communal change room who may expect to be observed by another person who is also changing, but may not expect to be recorded: Criminal Code (Qld) s 227A(1), note.

place' is a place where a person might reasonably be expected to be engaging in a private act.[188]

[2.120] It is also an offence to observe or visually record another person's genital or anal region (bare or covered by underwear), without consent and in circumstances where a reasonable adult would expect to be afforded privacy in relation to that region.[189]

[2.121] Where the observation or recording is of a person engaging in a private act or the person's genital or anal region, the offence applies if the observation or recording was made for the purpose of observing or visually recording that act or that region.[190]

[2.122] It is also an offence to distribute a recording of the kind described in [2.119] or [2.120] above without the person's consent. Such a recording is a 'prohibited visual recording'.[191]

Distribution of images or recordings

[2.123] The Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 proposes to amend the Criminal Code to insert two new offences dealing with intimate images and prohibited visual recordings.[192]

[2.124] Under the Bill, an 'intimate image' is defined to mean a moving or still image that depicts a person engaged in an intimate sexual activity not ordinarily done in public, or that depicts the person's bare breasts or genital or anal region (bare or covered only by underwear).[193]

---

188 Criminal Code (Qld) s 207A (definitions of 'private act' and 'private place'). The term 'state of undress' is defined to mean that the person is naked or their breasts or genital or anal region is bare, the person is wearing only underwear, or the person is wearing only some outer garments so that some underwear is not covered: s 207A.

189 Criminal Code (Qld) s 227A(2), (3).

190 Criminal Code (Qld) s 227A(1)(a), (b)(ii), (2)(b). This requirement does not apply to the observation or visual recording of a person in a private place.

191 Criminal Code (Qld) s 227B(1). The offence applies if the person who distributes the recording has reason to believe that it is a prohibited visual recording.

192 Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 (Qld) cll 5, 9 inserting new ss 223 and 229A (maximum penalty three years imprisonment). The Bill was introduced into Parliament on 22 August 2018. See the Legal Affairs and Community Safety Committee, Parliament of Queensland, *Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018*, Report No 20 (October 2018) which recommended that the Bill be passed.

The Bill also provides for a court to make a 'rectification order', which requires a convicted person to take reasonable action to remove, retract, recover, delete or destroy an image or recording. A failure to comply with the order is punishable by up to two years imprisonment: cl 9.

193 Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 cl 4(1) amending s 207A. The term also includes an image that has been altered to appear to show one of those things, or an image that depicts one of those things but has been digitally obscured if the person is depicted in a sexual way. The term 'prohibited visual recording' is defined consistently with s 227B as described at [2.122] above: cl 4(1) amending s 207A.

[2.125] With some exceptions,[194] it would be an offence to distribute an intimate image of another person, without that other person's consent and in a way that would cause that person distress reasonably arising in all the circumstances.[195]

[2.126] It would also be an offence to threaten to distribute an intimate image or a prohibited visual recording, without the consent of the depicted person and in a way that would cause distress reasonably arising in all the circumstances. The offence would apply if the threat is made in a way that would cause fear, reasonably arising in all the circumstances, of the threat being carried out.[196]

[2.127] Legislation in most other Australian jurisdictions also contains similar provisions that prohibit observing or recording another person in breach of privacy, and distributing or threatening to distribute images or recordings of a similar nature.[197]

Other offences

[2.128] There are also other offences that might apply.

[2.129] The offence of unlawful stalking in chapter 33A of the Criminal Code can involve watching a person, watching a place where a person lives, works or visits or following a person.[198] The conduct must be intentionally directed at a person, and can be conduct that is engaged in on one protracted occasion or on multiple occasions.[199] The commission of this offence could involve the use of surveillance devices.

[2.130] It is an offence to take an indecent photograph or record, by means of any device, an indecent visual image of a child under 16 years of age.[200]

[2.131] It is also an offence to engage in computer hacking or misuse. Where access to or use of a computer is restricted (for example, by requiring a code), it is an offence to use that computer without the consent of the person who has a right to control its use. The 'use' of a computer includes accessing or altering information

---

194 Specifically, it is a defence to show that a person's conduct was for a genuine artistic, educational, legal, medical, scientific or public benefit purpose and was, in the circumstances, reasonable for that purpose: Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 cl 5 inserting new s 223(4).

195 Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 cl 5 inserting new s 223. The term 'consent' is defined as consent freely and voluntarily given by a person with the cognitive capacity to give consent, but a child under 16 is incapable of giving consent. Examples of relevant circumstances include the circumstances surrounding the distribution, the extent to which the distribution interferes with the other person's privacy and the relationship between the person who distributed the image and the other person.

196 Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 cl 9 inserting new s 229A. See n 186 above as to 'consent'. Examples of relevant circumstances include the circumstances surrounding the threat and the relationship between the persons involved.

197 See, eg, *Crimes Act 1900* (ACT) s 61B and pt 3A; *Crimes Act 1900* (NSW) pt 3 divs 15B, 15C; Criminal Code (NT) pt VI div 7A; *Summary Offences Act 1953* (SA) pt 5A; *Police Offences Act 1935* (Tas) ss 13A–13D; *Summary Offences Act 1966* (Vic) pt 1 div 4A. In Western Australia, similar legislation is currently before Parliament: Criminal Law Amendment (Intimate Images Bill) 2018 (WA).

198 Criminal Code (Qld) s 359(c)(i), (iii).

199 Criminal Code (Qld) s 359(a), (b). See also the discussion in QLRC, *Review of termination of pregnancy laws*, Report No 76 (2018) [5.11]–[5.14].

200 Criminal Code (Qld) s 210(1)(f).

stored in the computer, or communicating information directly or indirectly to or from the computer. The offence may be aggravated if it involves causing detriment or gaining a benefit.[201]

[2.132] The use of surveillance might also involve trespass. At present, the *Invasion of Privacy Act 1971* includes specific provision making it an offence to enter a dwelling house without the consent of the owner or occupier,[202] or to gain entry by force, threats, intimidation, deceit or fraudulent means,[203] unless the entry was authorised, justified or excused by law or was made to protect the house or a person inside.[204] General offences of trespass apply under the *Summary Offences Act 2005* and the Criminal Code.[205]

Common law

[2.133] In limited circumstances, a number of common law actions may indirectly protect against surveillance by protecting other interests, such as those in property.

[2.134] An individual who has a right to exclusive occupation of land or premises may bring an action in trespass where there is an intrusion onto property.[206] It has been suggested that an intrusion into the airspace above land if it is at a height that is 'potentially necessary for the ordinary use and enjoyment of the occupier' might constitute a trespass.[207] It has also been suggested that, as a 'physical interference' with land or airspace is required, this action will 'not apply to a person who merely

---

201 Criminal Code (Qld) s 408E. In other jurisdictions, see: Criminal Code (ACT) pt 4.2; *Crimes Act 1900* (NSW) pt 6; Criminal Code (NT) pt VII div 10; *Criminal Law Consolidation Act 1935* (SA) pt 4A; Criminal Code (Tas) ch XXVIIIA and *Police Offences Act 1935* (Tas) pt VA; *Crimes Act 1958* (Vic) pt I div 3 subdiv 6; Criminal Code (WA) ch XLIVA; Criminal Code (Cth) ch 10 pt 10.7.

202 *Invasion of Privacy Act 1971* (Qld) s 48A(1). It is also an offence to be found in a dwelling house or the yard of a dwelling house without lawful excuse: s 48A(3). Those offences are punishable on summary conviction by a fine of up to 20 penalty units or imprisonment for one year.

203 *Invasion of Privacy Act 1971* (Qld) s 48A(2), punishable on summary conviction by a fine of up to 30 penalty units or imprisonment for 18 months.

204 Entry by threats, intimidation, deceit or fraud is not excused: s 48A(2)(a). Section 48A was intended to provide protection 'from forcible or deceptive entry by private inquiry agents or by repossession agents': Queensland, *Parliamentary Debates*, Legislative Assembly, 1 April 1976, 3330 (WE Knox, Minister for Justice and Attorney-General). The control of private inquiry agents and credit reporting agents, which was previously dealt with under the *Invasion of Privacy Act 1971* (Qld), is regulated under different legislation: see, respectively, the *Security Providers Act 1993* (Qld) and *Fair Trading Inspectors Act 2014* (Qld); *Privacy Act 1988* (Cth) pt IIIA.

205 See *Summary Offences Act 2005* (Qld) s 11, which makes it an offence to unlawfully enter or remain in a dwelling, a yard for a dwelling or a yard or place used for a business purpose (maximum penalty of 20 penalty units or imprisonment for one year); and Criminal Code (Qld) ss 421(1), 427(1), under which entry onto any premises, or unlawful entry of a vehicle, with intent to commit an indictable offence are crimes (maximum penalty 10 years imprisonment). See also Criminal Code ss 421(2), (3), 427(2) for more serious offences.

206 See generally *Plenty v Dillon* (1991) 171 CLR 635, 639 and the cases cited there; *Coco v The Queen* (1994) 179 CLR 427, 435; G Masel, H Grant and P Vout, Westlaw AU, *The Laws of Australia*, 'Trespass to Land' (1 June 2016) [33.8.470] ff; S Hinchcliffe, 'Drones—a "serious" invasion of privacy in the digital era?' (2014) 11(9) *Privacy Law Bulletin* 155, 157. An action in trespass does not protect a person who is visiting land, has hired premises for an event, or is 'in a public space and complains that there has been intrusion into his or her private activities, affairs or seclusion': ALRC Discussion Paper No 80 (2014) [3.36].

207 ALRC Discussion Paper No 80 (2014) [3.38]–[3.39]; Hinchcliffe, above n 206, 157; D Handel, 'The clouds have eyes—protecting privacy in the drone age' (2017) 14(4) *Privacy Law Bulletin* 63, 64–5 citing *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] 1 QB 479, 488–89.

follows or watches or keeps a person under surveillance without any threat, or who remains outside the land to carry out surveillance'.[208]

[2.135] An owner or occupier of land[209] is entitled to the quiet use and enjoyment of that land, and a person who substantially and unreasonably interferes with that entitlement may be liable in nuisance.[210] It has been suggested that an unreasonable interference may relevantly include 'keeping the occupier under surveillance', or 'positioning cameras or lights in situations where they interfere with, record or "snoop" on the occupier's activities'.[211]

[2.136] An action for breach of confidence can protect against the misuse or disclosure of 'confidential information'[212] where:[213]

- the confidential information is specifically identified;
- the information has the necessary quality of confidence, meaning it must not be common knowledge, in the public domain or be 'trivial tittle-tattle';

---

208 ALRC Discussion Paper No 80 (2014) [3.35]. An action in trespass to the person can also be satisfied by a threat of physical interference: [3.33], [3.35]. See also Hinchcliffe, above n 206, 157.

209 Only a person with an interest in land or a right to occupy or exclusively possess land may bring an action in nuisance. This may include an owner or lessee, but not another affected person, such as a person who is only visiting the land: see generally D Rolph, LexisAdvance, *Halsbury's Laws of Australia*, 'Private Nuisance' (21 March 2018) [415-640].

210 Ibid [415-620] ff.

211 ALRC Discussion Paper No 80 (2014) [3.37]; Hinchcliffe, above n 206, 157. See, eg, *Raciti v Hughes* (1995) 7 BPR 97,601 which concerned the use of sensor-activated lights and surveillance cameras aimed at the plaintiff's backyard.

It was stated in *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] 1 QB 479, 489 (Griffiths J) that:

> if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity … [the court may] regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief. However, that question does not fall for decision in this case and will be decided if and when it arises.

It has been observed that the 'intrusion' or 'interference' associated with actions in trespass and nuisance might be difficult to prove with respect to the use of some surveillance devices. For example, a camera might be used without entry onto land and an RPA might operate without intrusion or unreasonable interference: see, eg, Handel, above n 207, 64–5; Joint Working Group Report (2003) 349.

212 'Confidential information' has been generally described as 'information which is not generally or publicly known but is only known to a deliberately restricted number of individuals', and as extending to 'information respecting the personal affairs and private life of the plaintiff, and the activities of eavesdroppers and the like': see, respectively, ALRC Discussion Paper No 80 (2014) [3.43]; and *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255 (Gummow and Hayne JJ). See also T Lu, 'The protection of the private in public' (2015) 12(6) *Privacy Law Bulletin* 156, 158.

213 See P Bailey and S Churches, WestlawAU, *The Laws of Australia*, 'Breach of Confidence' (1 November 2013) [21.11.650]; Office of the Information Commissioner (Qld), *Annotated Legislation: Right to Information Act 2009 (Qld)—Breach of Confidence* (1 March 2012) <https://www.oic.qld.gov.au/annotated-legislation/rti/schedule-3/8-information-disclosure-of-which-would-found-action-for-breach-of-confidence/section-81/breach-of-confidence#>.

- the information was received in circumstances importing an obligation of confidence (having regard to what the person knew or ought to have known);[214] and
- there is an actual or threatened misuse of the information.[215]

Guidelines about surveillance

[2.137] Where a listening device or an optical surveillance device is not used in connection with a private conversation or activity, that use is generally not regulated by surveillance devices legislation. This might include, for example, the use of CCTV cameras on a street or in business premises for the purpose of security or community safety.[216]

[2.138] Some common users of surveillance devices in this context, such as government agencies, retail businesses or banks, may rely upon advisory guidelines, industry codes or standards, or internal policies and procedures to manage their use of surveillance.[217]

---

214 An 'obligation of confidence' may be imposed expressly or impliedly, by contract or by other circumstances, such as where personal details are imparted in a close personal relationship or where a party comes into possession of information which he or she knows, or ought to know, is confidential: Office of the Information Commissioner Queensland, *Annotated Legislation: Right to Information Act 2009 (Qld)—Breach of Confidence* (1 March 2012) <https://www.oic.qld.gov.au/annotated-legislation/rti/schedule-3/8-information-disclosure-of-which-would-found-action-for-breach-of-confidence/section-81/breach-of-confidence#>; ALRC Discussion Paper No 80 (2014) [3.44]–[3.45].

One commentator has stated, in relation to RPAs, that 'it seems probable that private information acquired by RPA would typically have a quality of confidence' and that the 'clandestine nature of RPA use could, depending upon the surrounding facts and circumstances, give rise to [an obligation of confidence]': Handel, above n 207, 65, considering *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255.

215 One commentator has stated that the requirement for actual or threatened misuse is a 'significant limitation', and observed that 'the action rests upon such misuse rather than the protection of privacy per se': Handel, above n 207, 65.

216 Additionally, that type of use may not be regulated by the *Information Privacy Act 2009* (Qld), because that legislation applies only to government agencies and if the surveillance captures 'personal information': see VLRC Report No 18 (2010) [3.17] and [2.104] ff above. The position may be different in New South Wales, where regulation of optical surveillance devices applies to all activities: see [2.74], [2.75] above, n 273 below.

217 See generally, VLRC Report No 18 (2010) [3.40]–[3.42], 57–8 Table 2; VLRC Consultation Paper No 7 (2009) [5.138]–[5.156]. See [2.111] above in relation to guidelines issued by the Office of the Information Commissioner (Qld). See also, eg, Transport and Infrastructure Senior Officials Committee, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for Mass Passenger Transport for Counter-Terrorism* (March 2012); Standards Australia, *Australian Standards: Closed Circuit Television (CCTV) Parts 1–4* (AS 4806.1–4806.4) (2006–2008).

Part 3: Issues for consideration

Introduction

[3.1] The Commission's terms of reference require it to recommend whether Queensland should consider legislation to appropriately protect the privacy of individuals in the context of civil surveillance technologies, including to regulate the use of surveillance devices and the communication or publication of information derived from surveillance devices.[218]

[3.2] There are gaps, inconsistencies and uncertainties in the current regulation of surveillance devices, and of privacy more generally.[219]

[3.3] In Queensland, in particular, the *Invasion of Privacy Act 1971* is outdated and limited in its scope.[220] The Act restricts the use of listening devices to overhear, record, monitor or listen to private conversations. However, it does not prohibit or restrict the use of optical surveillance devices, data surveillance devices, tracking devices or other surveillance devices.

[3.4] The shortcomings of the Act strongly suggest that a more comprehensive legislative response to the modern techniques of surveillance is required, both as to the range of devices and technologies that should be regulated and the range of activities that should be protected as private.

[3.5] In 2014, a Commonwealth Parliamentary Committee conducting an inquiry into drones reported that the range and complexity of laws relevant to surveillance and privacy creates uncertainty as to the scope of the law and its ability to cope with current technology, and that the lack of clarity may make it difficult for people to make a complaint and obtain adequate redress when they believe their privacy has been invaded. It was noted in particular that the increasing use and capability of technology such as drones increases the likelihood that there will be breaches of privacy.[221]

[3.6] The other laws of relevance to surveillance and privacy that apply in Queensland are inadequate. They are fragmented and, in some instances, apply differently to individuals and corporations.

[3.7] Existing State and Commonwealth information privacy legislation applies in limited circumstances and does not generally protect the privacy of individuals against surveillance. In particular, the Acts collectively:

---

218 The terms of reference are set out in full in Appendix A.

219 See, eg, Eyes in the Sky Report (2014) [4.24]–[4.28], [4.29] ff; C Robertson, 'CASA's new drone regulations highlight the need for more robust privacy laws in Australia' (2017) 14(3) *Privacy law Bulletin* 48, 49. See generally the discussion at [2.61] ff and [2.86] ff above.

220 Commonwealth legislation about telecommunications is also limited in scope, applying largely to the interception of communications as they are being transmitted from one person to another: see [2.89] ff above.

221 Eyes in the Sky Report (2014) [4.23]–[4.28].

- apply only to the collection and use of 'personal information';[222]
- apply primarily to government agencies and a limited class of other entities;[223]
- do not apply to all businesses, or to individuals acting in a private capacity;[224] and
- offer individuals a 'right to complain' but not a 'right of action' for a privacy breach—in general terms, although steps are to be taken within organisations to address a privacy issue, individuals whose privacy is breached will not ordinarily receive compensation or other similar remedy.[225]

[3.8] Criminal offences that may apply where a person breaches another person's privacy apply only in particular circumstances. Further, they operate to punish conduct after it occurs and do not regulate or prohibit the use of a surveillance device that may be relevant to such conduct.

[3.9] Whilst there are some common law actions that might indirectly protect a person's privacy, they are not intended to specifically address breaches of privacy and 'only provide piecemeal, limited protection'.[226]

[3.10] In most other Australian jurisdictions, surveillance devices legislation has been modernised and, in particular, has been updated to include regulation of optical surveillance devices, data surveillance devices and tracking devices.[227]

Preliminary view

[3.11] Considering the gaps, inconsistencies and uncertainties in the current legal framework in Queensland, the Commission considers that a new legislative framework to protect the privacy of individuals in the context of the use of civil surveillance devices and technologies is necessary.

[3.12] The legislation should be sufficiently broad in its scope to regulate existing and emerging surveillance technologies and strike a balance between the interests in the use of surveillance and the privacy rights and interests of individuals who may be harmed or affected if surveillance is unreasonably intrusive.[228] It should also aim

---

222 See, eg, A Allgrove and L Grimwood-Taylor, 'Privacy in the drone era: applying the Privacy Act to new technologies' (2016) 13(2) *Privacy Law Bulletin* 32, 35; Eyes in the Sky Report (2014) [4.12]. See also further discussion in A Hutchens and J Perier, 'Privacy in the digital era: the case for reform' (2017) 14(1) *Privacy Law Bulletin* 10, 10–11; VLRC Report No 18 (2010) [3.15].

223 See, eg, Handel, above n 207, 63–4.

224 See, eg, Eyes in the Sky Report (2014) [4.10]–[4.11]; Hutchens and Perier, above n 222, 11; Robertson, above n 219, 49; Handel, above n 207, 63–4; Hinchcliffe, above n 206, 156.

225 See, eg, Allgrove and Grimwood-Taylor, above n 222, 35; Hutchens and Perier, above n 222, 11.

226 Allgrove and Grimwood-Taylor, above n 222, 35. See also, eg, Handel, above n 207, 64–5.

227 The Australian Capital Territory and Tasmania are the other two remaining jurisdictions in which legislation is limited in scope to listening devices. However, it was recently recommended that the legislation in the Australian Capital Territory should be 'amended to include restrictions on other forms of surveillance activity, including visual observation, tracking and data collection': ACT Review (2016) [2.5](a). See also [D.23] ff below.

228 See [2.100]–[2.102] above, in relation to the Human Rights Bill 2018 (Qld).

to achieve reasonable consistency with the regulation of civil surveillance in other Australian jurisdictions.

Scope of a new legislative framework

[3.13] The form and scope of any new legislative framework to regulate surveillance in Queensland will depend on a number of underlying conceptual issues.

Surveillance as deliberate monitoring

[3.14] The Commission takes as the starting point that the legislation is concerned with regulating the use of surveillance devices in the context of civil surveillance (of individuals by other individuals, organisations or agencies). The widely accepted meaning of 'surveillance' in this context is the deliberate monitoring of a person, a group of people, a place or an object for some purpose, usually to obtain certain information about the person who is the subject of the surveillance, whether it occurs once or as part of a systematic activity.[229] Central to this is the notion of deliberate monitoring. Accordingly, inadvertent actions are generally not captured.[230]

Protecting individuals' reasonable expectations of privacy

[3.15] The Commission also considers that the focus and intent of the legislation should be on protecting the privacy of individuals from unjustified intrusions and interference. Specifically, the legislation should regulate surveillance by reference to reasonable expectations of privacy; surveillance is a part of everyday life and not all surveillance should be restricted. A challenge for the legislation is the recognition that expectations of privacy will differ depending on the context.[231]

Private conversations and activities

[3.16] The regulation of a listening device or optical surveillance device is linked to the concept of a 'private conversation' or a 'private activity'. In most jurisdictions, this does not include a conversation or activity carried on in circumstances where one or all of the parties should reasonably expect that it might be overheard, observed or recorded.[232]

[3.17] However, limiting the scope of legislation to a private conversation or activity might exclude from protection other information about which an individual also holds a reasonable expectation of privacy. This includes the location of a person or their property, and data obtained from their use of computerised systems. In other jurisdictions, the surveillance devices legislation treats the use of tracking devices and data surveillance devices differently from other forms of surveillance.[233]

[3.18] In relation to a tracking device, the infringement of privacy that is protected against is the use of a device to determine a person's geographical location. For example, the fact that a person is walking on a particular street at a particular time is

---

229 See the terms of reference in Appendix A. The use of surveillance devices for State law enforcement purposes is excluded from this review. Workplace surveillance is the subject of a separate review.

230 See [2.22]–[2.23] above. See also the discussion of 'intention or knowledge' at [3.58]–[3.62] below.

231 See [2.13] above

232 See [2.64], [2.75]–[2.76] above.

233 See [2.72], [2.74] and cf [2.75] above.

information available to passers-by, but the act of using a surveillance device for the purpose of tracking that person's movements is ordinarily considered an intrusion into the person's life.[234]

[3.19] On the other hand, there is a risk in widening the scope of the legislation, particularly in relation to the collection of data. Data surveillance is regulated only in a few jurisdictions and in particular circumstances.[235] It has been observed that 'the large number of legitimate uses for data surveillance makes it unreasonable to criminalise all use'.[236] Especially in the context of 'big data', data privacy overlaps with but also extends beyond the concept of surveillance as understood by surveillance devices legislation.[237]

Surveillance in public places

[3.20] The dividing line between public and private places is not always clear, but it is apparent that it gives rise to different expectations of privacy.[238] This is a matter of degree: it is reasonable for a person to expect a high degree of privacy, especially from outsiders, inside their home and to some extent within their backyards, but less so on the street outside their home; they might also expect a high level of privacy when using a public bathroom but less so when they are walking through a public park or shopping centre.

[3.21] The purposes and interests of surveillance users will also sometimes differ between public and private surveillance. Public place surveillance will often involve considerations of security and public safety.

[3.22] A consideration in this review is the extent to which the legislation might need to regulate public place surveillance differently. For example, the VLRC's review, which focused on public place surveillance, proposed a regulatory approach centred primarily on legislative principles, education and best practice guidance.[239]

---

234 See ACT Review (2016) [6.8]:

> the use of a device to locate the geographical location of a person or object in itself is considered an invasion of privacy and freedom of movement. The harm that comes from not being able to exercise choice as to your movement between public and private spaces is itself sufficient to give rise to the need for protection. Therefore, those jurisdictions where use of tracking devices is prohibited generally do not require any additional link with privacy interests.

235 See [2.74] above and Appendix B. Data surveillance devices are included in the surveillance devices legislation in New South Wales and South Australia and, in relation to use by law enforcement officers only, in the Northern Territory and Victoria.

236 Explanatory Statement, Surveillance Devices Bill 2007 (NT) cl 14. In the Northern Territory, the law about data surveillance devices was narrowed to apply only to law enforcement officers for this reason. An example given of legitimate use that should not be subject to surveillance legislation is parents and teachers monitoring the use of a computer by a child: Northern Territory, *Parliamentary Debates*, Legislative Assembly, 20 June 2007, 4760 (S Stirling, Justice and Attorney-General).

237 See [2.19] n 43, [2.29], [2.44], [2.48] above.

238 See, eg, ACT Review (2016) [6.7] in which it is suggested that the use of surveillance devices in public places 'will generally not give rise to privacy concerns'.

239 See [D.11] ff below. See also [3.286] ff below as to different enforcement and regulatory mechanisms.

Surveillance conducted covertly

[3.23] A related consideration is the extent to which the legislation might need to distinguish between overt and covert surveillance.[240] For example, the NSWLRC's proposed legislative scheme provided for different levels of oversight and regulation on the basis of this distinction, including a set of legislative principles to govern overt surveillance.[241]

[3.24] By its nature, covert surveillance involves a significant intrusion on an individual's privacy. Reasonable expectations of privacy may depend, in part, on the extent to which surveillance is conducted openly or in secret; covert surveillance is likely to attract much greater concern, even in situations in which surveillance might otherwise be tolerated. For example, depending on the purpose of the surveillance, the open use of a home security camera by a neighbour might be viewed differently from the use of hidden cameras by the same neighbour.

[3.25] Conversely, the greater the expectation of privacy in a given situation, the less acceptable covert surveillance will ordinarily be. For example, the use of a hidden recording device inside a person's home is likely to cause much greater concern than the use of visible CCTV cameras in public streets, especially where the expectation of privacy is balanced with an expectation of public safety.

[3.26] Covert surveillance may, nonetheless, be justified in limited circumstances. Identifying and providing for those circumstances will be a key consideration in the review.

Surveillance should ordinarily be done with consent

[3.27] Legislation usually treats surveillance and the collection of personal information about an individual as an infringement of the person's privacy unless the person consents to it.[242] As a general principle, surveillance should ordinarily be permitted if it occurs with consent. This is consistent with the approach in other jurisdictions.[243]

[3.28] However, notions of consent—when it is considered valid, when it can be implied, the extent to which it should be informed—are challenged in an environment in which emerging technologies are adopted at a rapid pace and traditional methods for obtaining consent are not easily applied in practice. For example, how does one ensure that footage of a person captured by a remotely piloted drone is obtained with consent, or that consent is obtained for surveillance of a large group of people?

---

240 See [2.24] above.

241 See [D.5] ff below.

242 See generally [2.68], [2.81], [2.106]–[2.107] above and Appendix B. Privacy is regarded as the interest a person has in controlling the extent to which information about them is conveyed to or is accessible by others: see [2.2], [2.5] above.

243 See generally [2.70] ff, [2.81] above and Appendix B. See also the discussions of consent as an exception to the use prohibition and the communication or publication prohibitions at [3.66] ff, [3.169] ff below.

Approaches to defining surveillance devices

[3.29] Finally, a fundamental question for the review is what approach should be taken to defining surveillance devices.

Recognised categories approach

[3.30] As explained above, the current approach of surveillance devices legislation in other jurisdictions is to regulate recognised categories of surveillance devices (that is, a listening device, optical surveillance device, tracking device or data surveillance device).[244]

[3.31] These categories are defined by reference to their general function or capability (for example, a device that can be used to listen, record, record visually, monitor or observe). In some jurisdictions a surveillance device also includes a combination of any two or more of those devices, or a device prescribed by regulation.[245] This approach provides 'some flexibility for changing technology' by enabling new devices to be prescribed in the future.[246]

[3.32] There is a risk that this approach could result in inconsistent and incomplete coverage and be outpaced by further technological developments (for example, in the area of biometric surveillance). Its effectiveness requires ongoing monitoring by the legislature.[247] On the other hand, it would capture commonly used and recognised categories of surveillance devices and provide certainty as to the scope of regulation and what needs to be done to comply with it.[248] It would also be consistent with the surveillance devices legislation in other jurisdictions and with the approach taken to surveillance devices used by law enforcement.[249]

Alternative technology neutral approaches

[3.33] Several law reform commissions and other bodies have noted that it is desirable for surveillance devices legislation to be 'technology neutral' or 'non-device specific', in order to keep pace with current and emerging technologies.[250]

---

244 See [2.72] above.

245 See [2.73] above.

246 Joint Working Group Report (2003) 367. See also 347.

247 See, eg, C Reed, 'Taking sides on Technology Neutrality' (2007) 4(3) *SCRIPT-ed* 264, 283–4 in which it is noted that 'specificity forces the lawmaker to reconsider the regulation at regular intervals'. That author identifies this as a potential benefit in 'ensuring that regulation keeps pace with technological and other changes'. See also P Ohm, 'The Argument against Technology-Neutral Surveillance Laws' (2010) 88 *Texas Law Review* 1685, 1686.

248 Ibid.

249 As to surveillance devices legislation that applies to law enforcement in Queensland, see [2.82] ff above.

250 See, eg, NSWLRC Report No 108 (2005) [1.8]; ALRC Report No 123 (2014) [14.32]; AAUS and Liberty Victoria Paper (2015) [4.2].

[3.34] There are different views about what a 'technology neutral' approach might look like.[251] On one view, it would focus on 'the nature of the activity subject to surveillance', rather than the technology that is being used.[252]

[3.35] The NSWLRC considered that surveillance and the use of a surveillance device defies technical limitations and precise delineations. In its view, any attempt to regulate surveillance through legislation limited to a few devices would inevitably be ineffectual. Instead, the NSWLRC recommended that 'surveillance device' should be defined broadly, to mean:[253]

> Any instrument, apparatus or equipment used either alone, or in conjunction with other equipment, which is being used to conduct surveillance.

[3.36] It also recommended that:[254]

> The [legislation] should define 'surveillance' as the use of a surveillance device in circumstances where there is a deliberate intention to monitor a person, a group of people, a place or an object for the purpose of obtaining information about a person who is the subject of surveillance.
>
> The [legislation] should define 'monitor' (as used in the definition of surveillance) as listening to, watching, recording, or collecting (or enhancing the ability to listen to, watch, record or collect) words, images, signals, data, movement, behaviour or activity.

[3.37] The NSWLRC recognised that those definitions are circular.[255] It also recognised that this approach would have the effect of capturing all activity that meets those broad definitions, unless specifically excluded.[256] It explained that '[t]he important factor will be whether the use of any device amounts to surveillance as defined by the legislation'.[257]

---

251 As a matter of degree, the existing recognised categories approach is sometimes described as 'technology neutral' or 'non-device specific' in that it applies to widely defined categories of devices without being limited to specific types of technologies: see, eg, Eyes in the Sky Report (2014) [4.37], Rec 4 and Eyes in the Sky Report: Government Response (2016) 9. See also ACT Review (2016) [6.4]; ALRC Report No 123 (2014) [14.39].

252 See ACT Review (2016) [6.4]–[6.5], in which it was also noted, with respect to the ALRC's approach, that it is 'the underlying privacy interest in question [that should] be protected against interference rather than use of particular devices'.

253 NSWLRC Interim Report No 98 (2001) [2.15]–[2.19], [2.33]–[2.36], Rec 1, endorsed in NSWLRC Report No 108 (2005), but not implemented.

254 NSWLRC Interim Report No 98 (2001) [2.37]–[2.39], Recs 2, 3.

255 See NSWLRC Report No 108 (2005) [1.8], [3.4], in which the NSWLRC explained that the definitions are 'deliberately circular so as to exclude the use of a surveillance device for purposes other than conducting surveillance':

> For an activity to constitute surveillance it must comprise the following elements: (1) the use of a surveillance device (2) where there is a deliberate intention to monitor a person, place, etc (3) for the purpose of obtaining information about the surveillance subject.

256 NSWLRC Interim Report No 98 (2001) [2.42].

257 NSWLRC Interim Report No 98 (2001) [2.40]. The NSWLRC suggested that the legislation would not apply to the use of surveillance devices for activities such as recreational photography (for example, filming at a wedding or a child's birthday party) or the taping of a lecture by a student, 'because their purpose is not to obtain information about the subjects of the surveillance … but merely to record an occasion for later enjoyment or as an aid to memory'. In their view, it also would not apply to everyday news-gathering activity, as something more is required than 'capturing the scene': NSWLRC Report No 108 (2005) [3.4]–[3.8]; NSWLRC Interim Report No 98 (2001) [3.4], [3.19].

[3.38] A similarly broad approach to defining 'surveillance device' was proposed by the AAUS and Liberty Victoria.[258]

[3.39] The ALRC also considered that surveillance devices legislation should be 'technology neutral', so that it can 'more readily be applied to any existing or emerging technology that could be used for surveillance'.[259] However, the ALRC did not recommend particular technology neutral definitions. It considered that the surveillance devices legislation should, at least, define 'surveillance device' to include the types of devices recognised under existing laws; that is, a listening device, optical surveillance device, tracking device or data surveillance device. It also considered that the legislation should 'apply to technologies that may be considered to fall outside the ordinary meaning of "device", such as software or networked systems'.[260]

[3.40] The ALRC noted that, given this approach, the offences would need to be appropriately tailored so that:[261]

> an offence would only be made out where the particular use of the device is inappropriate.

[3.41] On the one hand, it is suggested that a broad, technology neutral approach would ensure that the law is not outpaced by technological developments, eliminate the 'arbitrary gaps and regulatory anomalies' caused by device specific laws, and extend the protection of privacy to 'as wide a range of activity as reasonably possible'.[262]

[3.42] On the other hand, such an approach incorporates a degree of ambiguity[263] and may 'fail to capture important distinctions between different types of devices'.[264] There may be good reasons for treating certain devices differently, particularly given the diversity and ubiquity of technologies and the highly complex and nuanced nature of privacy.[265] This approach also carries the risk of over-inclusiveness, and would make many everyday activities, which are not presently regulated, the subject of

---

258 AAUS and Liberty Victoria Paper (2015) [4.2], Rec 2 which recommended that 'surveillance device' be defined broadly to mean 'any device capable of being used to':

(a) monitor, observe, overhear, listen to or record an activity; or

(b) determine or monitor the geographical location of a person or an object.

259 ALRC Report No 123 (2014) [14.32], Rec 14-2.

260 Ibid [14.32], [14.39].

261 Ibid [14.41].

262 See, eg, NSWLRC Interim Report No 98 (2001) [2.40]. See also [2.17].

263 Reed, above n 247, 266–68. See also Ohm, above n 247.

264 ALRC Report No 123 (2014) [14.37], referring to a submission by the Australian Privacy Foundation that:

> there may well be particular technologies which give rise to specific concerns. Where this is the case, or where it is necessary to avoid doubt about whether or not a type of device is subject to the law, there may be an inescapable need for definitions to refer to particular technologies.

265 Ohm, above n 247, 1695–96 in which it is noted that the critical principle in developing a practical approach to regulating surveillance should be to '[t]reat similar technologies alike and differing technologies differently'.

regulation and potential criminal liability.[266] Consequently, the legislation would need to be carefully drafted to exclude all permitted uses.

[3.43] It has long been recognised that privacy needs continually shift in the face of changing technologies.[267] Any area of regulation affected by technological developments will face the difficulty of dealing with a moving target. Legislation cannot predict all changes and will invariably require revision and updating.

[3.44] The recommendations made by the NSWLRC and the ALRC that a technology neutral approach be adopted were not included in draft legislation and have not been implemented.

[3.45] Where jurisdictions have reformed their surveillance devices legislation, the existing recognised categories approach has been retained, with improvements to expand the range of categories beyond listening devices and to modernise other aspects of the legislation.[268] This approach was also recommended in the recent ACT Review.[269]

Questions

Q-1 What considerations should apply to surveillance that is conducted in a public place?

Q-2 What considerations should apply to surveillance that is conducted overtly or covertly?

Q-3 Should new legislation adopt the existing 'categories' approach used in other jurisdictions and define 'surveillance device' to mean:

- **(a) a listening device;**
- **(b) an optical surveillance device;**
- **(c) a tracking device;**
- **(d) a data surveillance device;**
- **(e) other device (and if so, what should this be)?**

Q-4 If 'yes' to Q-3:

- **(a) how should each category of device be defined?**

266 See, eg, Ohm, above n 247, 1686, 1697–98.

267 For example, in its 1983 Report, the ALRC stated that legislation is 'not always the most appropriate to protect privacy interests' and noted that there is a role for other more flexible mechanisms, such as codes and guidelines: ALRC Report No 22 (1983) vol 2, [1069].

268 See, eg, the *Surveillance Devices Act 2007* (NSW) which replaced the *Listening Devices Act 1984* (NSW). See also [2.71] n 108 above.

269 ACT Review (2016) [2.5](a), [6.5].

(b) should each category of device be defined to extend to any particular technologies, such as a program or system?

(c) should 'surveillance device' also include:

(i) a combination of any two or more of those devices or technologies; or

(ii) any other device or technology prescribed by regulation?

Q-5 Alternatively to Q-3, should new legislation adopt a 'technology neutral' approach and define 'surveillance device' to mean, for example, 'any instrument, apparatus, equipment or technology used either alone, or in combination, which is being used to deliberately monitor, observe, overhear, listen to or record an activity; or to determine or monitor the geographical location of a person or an object', or some other definition?

The use of surveillance devices

[3.46] Surveillance devices legislation is intended to protect privacy by limiting the use of surveillance devices to circumstances that are justifiable. In broad terms, such legislation prohibits the use (or the installation, maintenance or attachment) of a surveillance device for certain purposes (the 'use prohibition') and is subject to particular exceptions.[270]

Installation, use, maintenance and attachment of surveillance devices

[3.47] In Queensland, the *Invasion of Privacy Act 1971* provides that:[271]

> A person is guilty of an offence against this Act if the person uses a listening device to overhear, record, monitor or listen to a private conversation and is liable on conviction on indictment to a maximum penalty of 40 penalty units or imprisonment for 2 years.

[3.48] Similar provisions are included in the surveillance devices legislation in other jurisdictions. In general, they provide that it is an offence for a person to use, install, maintain or attach:[272]

- a listening device to overhear, record, monitor or listen to a 'private conversation';
- an optical surveillance device to monitor, record visually or observe a 'private activity';[273]
- a data surveillance device to access, track, monitor or record information that is input into, output from or stored in a computer; or
- a tracking device to determine the geographical location of a person or object.

[3.49] A private conversation or activity is one that occurs in circumstances indicating that the parties do not want to be seen or heard by others, unless it is with their consent. It does not include a conversation or activity occurring in circumstances where the parties ought reasonably to expect that they might be seen or heard. A party generally includes a person who is speaking or being spoken to or participating in an activity, and sometimes a person who is present with consent.[274]

[3.50] These provisions are outlined in the following table:

---

270 This is one of the two principal types of prohibitions under surveillance devices legislation. As to the 'communication or publication prohibitions', see the discussion at [3.155] ff below.

271 *Invasion of Privacy Act 1971* (Qld) s 43(1).

272 *Listening Devices Act 1992* (ACT) s 4(1); *Surveillance Devices Act 2007* (NSW) ss 7(1), 8(1), 9(1), 10(1); *Surveillance Devices Act* (NT) ss 11(1), 12(1), 13(1), 14(1); *Surveillance Devices Act 2016* (SA) ss 4(1), 5(1), 7(1), 8(1); *Listening Devices Act 1991* (Tas) s 5(1); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1), 9(1); *Surveillance Devices Act 1998* (WA) ss 5(1), 6(1), 7(1).

273 The position is different in New South Wales, where the prohibition applies to any activity and is primarily concerned with consent for any interference with land, a vehicle or an object: *Surveillance Devices Act 2007* (NSW) s 8(1). The term 'activity' is not defined by the legislation.

274 See [2.66], [2.77]–[2.78] above.

	Qld (listening devices)	ACT (listening devices)	NSW (all devices)	NT (listening, optical and tracking devices)	SA (all devices)	Tas (listening devices)	Vic (listening, optical and tracking devices)	WA (listening, optical and tracking devices)
Use	✓	✓	✓*	✓	✓*	✓*	✓	✓*
Install			✓	✓	✓		✓	✓*
Maintain			✓	✓	✓		✓	✓*
Attach			✓	✓			✓	✓* (tracking only)
a listening device, in relation to a private conversation, to–								
Overhear	✓		✓		✓		✓	
Record	✓	✓	✓	✓	✓	✓	✓	✓
Monitor	✓		✓	✓	✓		✓	✓
Listen to[275]	✓	✓	✓	✓	✓	✓	✓	✓
an optical surveillance device, in relation to a private activity, to–								
Record visually			✓ (any activity)	✓	✓		✓	✓
Monitor				✓				
Observe			✓ (any activity)	✓	✓		✓	✓
a data surveillance device, in relation to information input into, output from or stored in a computer, to[276]**–**								
Access that information					✓			
Track that information					✓			
Monitor that information			✓ (in/output only)		✓			
Record that information			✓ (in/output only)		✓			
a tracking device, in relation to a person or object, to–								
Determine geographical location			✓	✓	✓		✓	✓

* The relevant legislation states that a person must not 'use or cause to be used' a listening device. In Tasmania, a person must also not 'permit' the use of a listening device. In Western Australia, the legislation extends to causing any device to be used, installed, maintained or attached.

275 In the Australian Capital Territory, the Northern Territory, Tasmania and Western Australia, the term 'listen to' is defined to include 'hear': *Listening Devices Act 1992* (ACT) Dictionary; *Surveillance Devices Act* (NT) s 4; *Listening Devices Act 1991* (Tas) s 3(1); *Surveillance Devices Act 1998* (WA) s 3(1).

276 The legislation in the Northern Territory and Victoria regulates the use of a data surveillance device for law enforcement officers only: *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9. Those provisions are not included in this table.

[3.51] As shown in the table above, the use prohibition in the surveillance devices legislation of many of the other jurisdictions differs in scope from the prohibition in Queensland. In particular, in many jurisdictions:

- the prohibition is not limited to listening devices and applies to other categories of surveillance device, such as an optical surveillance device;
- the prohibition applies to using a surveillance device, as well as to 'installing', 'maintaining' or 'attaching' such a device; and
- the prohibition extends to a person who causes or permits a surveillance device to be used.[277]

[3.52] The *Invasion of Privacy Act 1971* does not define 'use'. In some other jurisdictions the legislation states that 'use' of a surveillance device 'includes use of the device to record a conversation or other activity', but does not otherwise define the term.[278]

[3.53] The ordinary meaning of 'use' is broad and often variable, but relevantly includes putting something into action or service, or carrying out a purpose or action by means of a particular thing.[279]

[3.54] Some common examples of 'use' of a device might be a person using their mobile phone to make an audio recording of a face-to-face conversation with another person, or a person using a video camera to make an audio-visual recording of an event held at their house.

[3.55] In some jurisdictions, the term 'install' is defined to include 'attach', but those terms are otherwise not defined.[280]

[3.56] In those jurisdictions that have extended the prohibition to maintaining a surveillance device, the legislation defines 'maintain' to include adjusting, relocating or repositioning, repairing and servicing a surveillance device, or replacing a faulty device.[281]

---

277 The provisions vary: see *Surveillance Devices Act 2007* (NSW) s 7(1); *Surveillance Devices Act 2016* (SA) s 4(1); *Listening Devices Act 1991* (Tas) s 5(1); *Surveillance Devices Act 1998* (WA) ss 5(1), 6(1), 7(1).

278 See the definition of 'use' in *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; *Surveillance Devices Act 1999* (Vic) s 3(1).

279 *Merriam-Webster Dictionary* (online, 2018) <https://www.merriam-webster.com/dictionary/use>; *Oxford Dictionary* (online, 2018) <https://en.oxforddictionaries.com/definition/use>.

280 See the *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; and *Surveillance Devices Act 1999* (Vic) s 3(1) which define 'install' to include attach.

Cf the *Police Powers and Responsibilities Act 2000* (Qld) s 324A which states that 'a reference to the installation of a surveillance device includes a reference to doing anything to or in relation to a device to enable it to be used as a surveillance device'. That Act also states that examples of things that might be done are installing hardware or software on the device, or establishing a wireless connection between the device and another device.

281 See the definition of 'maintain' in *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; *Surveillance Devices Act 2016* (SA) s 3(1); *Surveillance Devices Act 1999* (Vic) s 3(1); *Surveillance Devices Act 1998* (WA) s 3(1).

[3.57] This might cover, for example, adjusting the angle of a CCTV camera positioned at a fixed location to change the scope of what is being recorded. It might also include upgrading the audio recording software on a tablet computer to enhance its recording range.

Intention or knowledge

[3.58] The use prohibition in other jurisdictions usually includes a mental element of knowledge or intent.

[3.59] In some instances, a person is prohibited from 'knowingly' installing, using, maintaining or attaching a device for a particular purpose,[282] or for a particular purpose without appropriate consent.[283]

[3.60] In other instances, a person is prohibited from using a device 'with the intention of' acting in a way that is prohibited.[284] Alternatively, some legislation states that a prohibition will not apply where a person's actions were unintentional.[285] In Queensland, the use prohibition does not apply to the unintentional hearing of a private conversation by means of a telephone.[286]

[3.61] The addition of a 'mental element' such as knowledge or intent limits the prohibition to deliberate conduct and adds to the difficulties of proof of the commission of the offence.

[3.62] For example, a person might commit an offence under the surveillance devices legislation if they install a web camera on their home computer for the purpose of secretly recording a private conversation taking place in their home. They might not commit an offence, however, if they install a web camera on their home computer to participate in an internet video conversation with another person, although the camera might inadvertently record other background conversations.

Exceptions: where use of a surveillance device is permitted

[3.63] In each jurisdiction, there are various exceptions to the use prohibition, as summarised in the table below:[287]

---

282 *Surveillance Devices Act 2007* (NSW) s 7(1); *Surveillance Devices Act 2016* (SA) s 4(1).

283 *Surveillance Devices Act 2007* (NSW) ss 8(1), 9(1), 10(1); *Surveillance Devices Act* (NT) ss 11(1), 12(1), 13(1), 14(1); *Surveillance Devices Act 2016* (SA) ss 5(1)–(3), 7(1), 8(1); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1), 9(1). As to consent, see also *Surveillance Devices Act 2016* (SA) s 4(2)(a)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(c),(d), 6(3), 7(1).

284 *Listening Devices Act 1992* (ACT) s 4(1).

285 *Listening Devices Act 1992* (ACT) s 4(2)(b); *Surveillance Devices Act 2007* (NSW) s 7(2)(c); *Surveillance Devices Act 2016* (SA) s 4(2)(f); *Listening Devices Act 1991* (Tas) s 5(2)(d); *Surveillance Devices Act 1998* (WA) ss 5(2)(e), 6(2)(e). Specifically, these actions relate to the unintentional hearing of a private conversation by means of a listening device, or the unintentional observation or recording of a private activity by means of an optical surveillance device.

286 *Invasion of Privacy Act 1971* (Qld) s 43(2)(b).

287 The table does not include exceptions that are specific to law enforcement. Limited information about exceptions applying to law enforcement officers is included where relevant in the discussion that follows.

	Qld (listening devices)	ACT (listening devices)	NSW (all devices)	NT (listening, optical and tracking devices)	SA (all devices)	Tas (listening devices)	Vic (listening, optical and tracking devices)	WA (listening, optical and tracking devices)
Consent of subject of surveillance[288]		✓ (recording by a party with consent of each principal party, with consent of one principal party to protect that party's lawful interests, or with consent of one principal party where recording is not for purpose of communication or publication to a non-party)	✓ (listening; recording by a party with consent of each principal party, with consent of one principal party to protect that party's lawful interests, or with consent of one principal party where recording is not for purpose of communication or publication to a non-party) (tracking: of a person, with consent of that person)	✓ (listening and optical; offence to use without consent of each party) (tracking: person, or person in possession/control of object)	✓ (listening; recording by a party with consent of each principal party) (optical; for use on premises, vehicle or thing, consent of each party is required. Consent for entry or interference to premises etc is also required) (tracking: of a person, with consent of that person)	✓ (recording by a party with consent of each principal party, with consent of one principal party to protect that party's lawful interests, or with consent of one principal party where recording is not for purpose of communication or publication to a non-party)	✓ (listening and optical; offence to use etc without consent of each party) (tracking: of a person, with consent of that person)	✓ (listening and optical; offence to use etc without consent of each party, or with consent of one principal party to protect that party's lawful interests) (tracking: of a person, with consent of that person)
Consent of another person			✓ (optical and data; for use etc on premises, vehicle or thing, or on computer or computer network, any entry or interference requires consent of owner, occupier or person in lawful control) (tracking: of an object, with consent of person in possession or control)		✓ (optical; for use etc on premises, vehicle or thing, any entry or interference requires consent of owner, occupier or person in lawful control. Consent of participants also required) (data; consent of owner, or person with lawful control or management, of computer) (tracking: of a vehicle or thing, with consent of person in possession or control)		✓ (tracking: of an object, with consent of person in possession or control)	✓ (tracking: of an object, with consent of person in possession or control)
Participant monitoring	✓ (offence not applicable if person is a party)			✓ (listening and optical; offence requires person is not a party)			✓ (listening and optical; offence requires person is not a party)	
Safety and well-being						✓ (imminent threat of serious violence, substantial property damage or serious narcotics offence)		✓ (listening and optical; on behalf of a child or protected person, where it is to protect their best interests and in the public interest)

288 For Queensland, the Australian Capital Territory, New South Wales, Tasmania and Western Australia, see also the definition of 'party', outlined at [2.66], [2.77]–[2.78] above.

	Qld (listening devices)	**ACT** (listening devices)	**NSW** (all devices)	**NT** (listening, optical and tracking devices)	**SA** (all devices)	**Tas** (listening devices)	**Vic** (listening, optical and tracking devices)	**WA** (listening, optical and tracking devices)
Lawful interests		✓ (recording by a party with consent of a principal party, to protect that party's lawful interests)	✓ (listening; recording by a party with consent of a principal party, to protect that party's lawful interests)		✓ (listening; recording by a party to protect their lawful interests) (listening or optical: installation on premises permitted to protect lawful interests)	✓ (recording by a party with consent of a principal party, to protect that party's lawful interests)		✓ (listening and optical; recording by a party with consent of a principal party, to protect that party's lawful interests)
Public interest				✓ (listening and optical; in an emergency)	✓ (listening and optical)			✓ (listening and optical; with consent of a principal party, on behalf of a child or protected person, or in an emergency)
Lawful purpose			✓ (tracking)					
Private investigator or loss adjuster					✓ (listening and optical: in course of functions and reasonably necessary to protect person's lawful interests, or in the public interest)			
Unintentional actions	✓ (unintentional hearing by telephone)	✓	✓ (listening)		✓ (listening)	✓		✓ (listening and optical)
Location and retrieval			✓ (listening and optical)		✓ (listening, optical and tracking)			
Prescribed circumstances				✓ (tracking)	✓			✓ (tracking)

[3.64] Many exceptions relate to use that is authorised by other law, matters of law enforcement or government use (for example, use by fire and emergency services).[289]

289 See, eg, *Invasion of Privacy Act 1971* (Qld) s 43(2)(c)–(e); *Listening Devices Act 1992* (ACT) ss 3B, 3C, 4(2)(a); *Surveillance Devices Act 2007* (NSW) ss 7(2)(a), (b), (d), (f), (4), 8(2)(a), (b), (d)–(f), 9(2)(a)–(b), 10(2), pts 3-6; *Surveillance Devices Act* (NT) ss 11(2), 12(2), 13(2), 14(2), 14A, pts 4–8; *Surveillance Devices Act 2016* (SA) ss 4(2)(b)(i)–(iii), (d), (e), 5(4)(a)(i)–(iii), (c), (d), 7(2)(a), 8(2)(a), pts 3–4; *Listening Devices Act 1991* (Tas) s 5(2)(a)–(ba), (e), pt 4; *Surveillance Devices Act 1999* (Vic) ss 6(2), 7(2), 8(2), 9(2), pts 4–5; *Surveillance Devices Act 1998* (WA) ss 5(2)(a)–(c), (3)(a)–(b), 6(2)(a)–(c), (3)(b)(i)–(ii), 7(2), pt 4.

The terms of reference exclude the use of surveillance devices for State law enforcement purposes from this review: see terms of reference, para E.

[3.65] Other exceptions apply more generally, for example, permitting a person to use a surveillance device with consent, to protect someone's safety or for a lawful purpose.

Use of a surveillance device with consent

[3.66] In most jurisdictions, the use of a surveillance device with consent is usually permitted. In most instances, this refers to the consent of the parties to a conversation or activity, or the person who is subject to the surveillance. In a few instances, the consent of another person, such as the owner of relevant premises, is required.

[3.67] 'Consent' may be express or implied,[290] but is not otherwise defined in surveillance devices legislation.

[3.68] The concept of 'implied consent' may be problematic because:[291]

- it may be difficult to determine whether consent can be implied in particular circumstances, and what the extent of any implied consent is;
- technological advances make it difficult to know if surveillance is occurring, which can alter expectations about privacy and impact on whether a person has been reasonably notified about and is consenting to surveillance; and
- consent may not be 'truly voluntary' where it is inconvenient or impossible for a person to choose not to be subject to surveillance.

[3.69] In the ACT Review, it was considered that consent should be 'clearly established'. It was recommended that consent should require that the person is adequately informed, provides consent that is 'current and specific', acts voluntarily and has the capacity to understand and communicate their consent.[292]

[3.70] In contrast, the VLRC concluded that the notion of implied consent:[293]

---

290 See, eg, *Invasion of Privacy Act 1971* (Qld) ss 42(2)(b), 43(2)(a); *Listening Devices Act 1992* (ACT) Dictionary (definition of 'consent'); *Surveillance Devices Act 2007* (NSW) ss 7(3)(a), 9(1), 10(1); *Surveillance Devices Act* (NT) ss 11(1)(b), 12(1)(b), 13(1)(b); *Surveillance Devices Act 2016* (SA) ss 4(2)(a)(i), 5(1)–(3); 7(1), 8(1); *Listening Devices Act 1991* (Tas) s 5(3)(a); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1); *Surveillance Devices Act 1998* (WA) ss 5(3)(c)–(d), 6(3)(a), 7(1).

291 ACT Review (2016) [2.5](e), [6.22]–[6.26], [6.30]; VLRC Report No 18 (2010) [6.15]–[6.23].

In reviewing privacy law, the ALRC observed that '[t]here is a pressing need for contextual guidance on consent' and that '[w]hat is required to demonstrate that consent has been obtained is often highly dependent on … context'. The ALRC concluded that it would be most appropriate for there to be guidance from the Privacy Commissioner, including about the factors to be considered in assessing whether consent has been obtained. The VLRC considered adopting this approach in Victoria, noting that there was support but also opposition from the police and the Privacy Commissioner: ALRC Report No 108 (2008) vol 1, [19.58] ff; VLRC Report No 18 (2010) [6.17]–[6.18].

292 ACT Review (2016) [2.5](e), [6.26], [6.30]. See also [6.23]–[6.25]; VLRC Report No 18 (2010) [6.15].

293 VLRC Report No 18 (2010) [6.21]. The VLRC emphasised the importance of providing adequate notice of surveillance, such as appropriate signage.

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.

Consent of persons subject to surveillance

[3.71] In some jurisdictions, the concept of consent is an integral part of the terms 'private conversation' and 'party'. Generally, a conversation may be private if the parties want it to be heard only by themselves and another person who has their consent, and a person may be a party to a conversation or activity if they are present to listen, observe or record (or similar) with the consent of the principal parties.[294]

[3.72] In most jurisdictions, a person is not prohibited from using a listening device or optical surveillance device to listen to, monitor, observe or record a private conversation or activity if that is done with the consent of the principal parties.[295] In some jurisdictions, this is expressed as an exception to the use prohibition for a party to a conversation or activity.[296] In other jurisdictions, a lack of consent is an element of the offence.[297]

[3.73] There are also some circumstances where the consent of only one principal party to a private conversation or activity is required. This includes, for example, the use of a device in a person's lawful interests or a recording that is not made for the purpose of communication or publication to a person who is not a party.[298]

[3.74] Where a tracking device is installed, used, maintained or attached to determine the geographical location of a person, it is a requirement to obtain that person's consent.[299]

Consent of another person

[3.75] In some jurisdictions, consent to install, use or maintain a surveillance device is required from another person.

---

294 See [2.64], [2.66], [2.75]–[2.78] above.

295 The effect of the participant monitoring provisions, discussed at [3.82] ff below, is that, for a person who is a party to a conversation or activity, consent to the use of a surveillance device is not required.

296 *Listening Devices Act 1992* (ACT) s 4(1), (3)(a); *Surveillance Devices Act 2007* (NSW) s 7(1), (3)(a); *Surveillance Devices Act 2016* (SA) ss 4(1), (2)(a)(i), 5(1); *Listening Devices Act 1991* (Tas) s 5(1), (3)(a); *Surveillance Devices Act 1998* (WA) ss 5(1), (3)(c), 6(1), (3)(a). In the Australian Capital Territory and Western Australia, a person may also use a device on behalf of a party in these circumstances.

With the exception of South Australia, the other jurisdictions, including Queensland, have a broader definition of 'party' that encompasses a person who overhears, listens to, monitors, or records a private conversation or activity with consent. In South Australia, 'party' is not defined, but there are other requirements for consent: see [3.75] ff below.

297 *Surveillance Devices Act* (NT) ss 11(1), 12(1); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1). These jurisdictions permit participant monitoring, meaning that the offence applies only where a person is not a party (and the term 'party' is limited only to those people who would be a 'principal party' to a conversation or activity).

298 *Listening Devices Act 1992* (ACT) s 4(3)(b); *Surveillance Devices Act 2007* (NSW) s 7(3)(b); *Listening Devices Act 1991* (Tas) s 5(3)(b); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii).

299 *Surveillance Devices Act 2007* (NSW) s 9(1); *Surveillance Devices Act* (NT) s 13(1); *Surveillance Devices Act 2016* (SA) s 7(1); *Surveillance Devices Act 1999* (Vic) s 8(1); *Surveillance Devices Act 1998* (WA) s 7(1).

[3.76] In New South Wales and South Australia, a person may install, use or maintain an optical surveillance device on or in premises, a vehicle or any other thing to observe or record an activity, only if:[300]

- for any entry onto or into premises[301] or a vehicle,[302] the owner or occupier has consented; or
- for any interference with premises, a vehicle or a thing, the person in lawful possession or control has consented.

[3.77] In New South Wales, this applies to any activity. In South Australia, it is restricted to a private activity and it is also necessary for the person to obtain the consent of each party to the activity.

[3.78] The position is similar for a data surveillance device, where the consent of a person using the computer is not required, but:[303]

- in New South Wales, for any entry onto or into premises or interference with a computer or computer network, the consent of the owner, occupier or person in lawful possession or control is required; and
- in South Australia, the consent of the owner, or the person with lawful control or management, of the computer is required for the installation, use or maintenance of a data surveillance device.

[3.79] A tracking device may be installed, used, maintained or attached to determine the geographical location of a vehicle or object only if it is with the consent of the person who is in lawful possession or control of that vehicle or object.[304]

[3.80] In New South Wales, it was explained that because these provisions operate on the basis of an entry or interference that is without consent, they 'will not capture people who have security devices in their own home or premises'.[305]

[3.81] Some examples of activity which is not captured might include:

---

300 *Surveillance Devices Act 2007* (NSW) s 8(1); *Surveillance Devices Act 2016* (SA) s 5(1)–(3).

301 'Premises' is defined to include land, a building, part of a building and any place whether built on or not, whether in or outside the jurisdiction: *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act 2016* (SA) s 3(1).

302 In New South Wales, the term 'vehicle' is defined to include an aircraft, a vessel or a part of a vehicle, whether in or outside of the jurisdiction. In South Australia, it includes any vessel or aircraft: *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act 2016* (SA) s 3(1).

303 *Surveillance Devices Act 2007* (NSW) s 10(1); *Surveillance Devices Act 2016* (SA) s 8(1). As the knowledge or consent of the person using the computer is not required, this might enable a person to monitor the activities of another person using a computer without the other person's knowledge or consent.

Legislation in the Northern Territory and Victoria is limited to law enforcement officers but requires the consent of the person about whom information will be obtained: *Surveillance Devices Act* (NT) s 14(1); *Surveillance Devices Act 1999* (Vic) s 9(1). See also NSWLRC Interim Report No 98 (2001) [2.106].

304 *Surveillance Devices Act 2007* (NSW) s 9(1); *Surveillance Devices Act* (NT) s 13(1); *Surveillance Devices Act 2016* (SA) s 7(1); *Surveillance Devices Act 1999* (Vic) s 8(1); *Surveillance Devices Act 1998* (WA) s 7(1).

305 New South Wales, *Parliamentary Debates*, Legislative Assembly (6 November 2007) 3579 (D Campbell, Minister for Police and Minister for the Illawarra). This explanation applies to the approach taken for an optical surveillance, data surveillance or tracking device.

- a person installing a security camera on their own home or a dashboard camera in their own car, and using that to record an activity without consent (but in South Australia, not a private activity);
- a person using a video camera to record a wedding held at a relative's home with the consent of the relative who owns or occupies the premises;
- a person installing and using a device on their own computer to keep track of when and how that computer is used by another person without the other person's consent.

Use of a surveillance device for participant monitoring

[3.82] In Queensland, the *Invasion of Privacy Act 1971* provides that the use prohibition does not apply 'where the person using the listening device is a party to the private conversation'.[306]

[3.83] The position is similar in the Northern Territory and Victoria. There, a person who uses a listening device or optical surveillance device to record a private conversation or activity to which they are a party is not required to advise the other parties of the recording or obtain their consent.[307]

[3.84] This is referred to as 'participant monitoring'.[308]

[3.85] In other jurisdictions, participant monitoring is prohibited, because a person may not record a private conversation or activity to which they are a party without the consent of the other parties.[309] There are, however, some limited legislative exceptions, including the use of a device in a person's lawful interests, in the public interest, for a person's safety or well-being or for a lawful purpose.[310]

[3.86] Various arguments have been made both in favour of, and against, participant monitoring. On the one hand, it has been observed that:[311]

- participant monitoring is a currently accepted practice used to protect a person's own interests, especially in commercial, business and domestic contexts;

---

306 *Invasion of Privacy Act 1971* (Qld) s 43(2)(a).

307 *Surveillance Devices Act* (NT) ss 11(1), 12(1); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1). The regulation of the use of optical surveillance devices in New South Wales, which does not require the consent of those being recorded, may also permit participant monitoring to occur: *Surveillance Devices Act 2007* (NSW) s 8(1).

308 See [2.65], [2.79] above.

309 *Listening Devices Act 1992* (ACT) s 4(1); *Surveillance Devices Act 2007* (NSW) s 7(1); *Surveillance Devices Act 2016* (SA) ss 4(1), 5(1); *Listening Devices Act 1991* (Tas) s 5(1); *Surveillance Devices Act 1998* (WA) ss 5(1), 6(1). See also the *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5(1) (definition of 'communication'), 6(1), 7(1) pursuant to which a person must not intercept a communication passing over a telecommunications system without the knowledge of the other person making the communication.

310 The exceptions are discussed at [3.106] ff below. See also NSWLRC Interim Report No 98 (2001) [2.99]; VLRC Report No 18 (2010) [6.59]–[6.69]; NZLC Report No 113 (2010) [3.80] ff.

311 ALRC Report No 22 (1983) vol 2, [1129]–[1135]; NSWLRC Interim Report No 98 (2001) app A.

- participant monitoring is permitted in other jurisdictions (or if restricted, contains broad exceptions) and there is no evidence of harmful social effects or a chilling effect;
- any person speaking to another takes a risk that the conversation will be recorded in some way or disclosed to others and the regulation of the use of a listening device does not remove that risk;
- a person may construct a record of a conversation from their notes or their own recollection, and should not be prevented from making a more accurate record where technology allows;[312]
- a prohibition on participant monitoring assumes that a conversation is confidential, but would criminalise a breach of that confidentiality only if it involved recording the conversation using a surveillance device;
- an agreement between the parties to a conversation to keep the conversation private is not necessarily breached by recording the conversation, but only by its disclosure;
- a prohibition on participant monitoring would not prohibit the disclosure of a private conversation that does not rely on a recording, nor would it prohibit others from denying or telling untruths about a conversation; and
- a prohibition on participant monitoring, with exceptions, does not have the effect of limiting the practice, because the exceptions are broadly expressed and do not provide a 'realistic legal barrier'.

[3.87] It has been argued, in particular, that for something to be a criminal offence there must be a clear public interest involved:[313]

> Reasonable expectations do not, of themselves, create such a public interest. The [right] of a person to make such recordings at present is a substantive legal right. There is no convincing reason given as to why this right is less important than the interest of the other individuals in controlling the mode of recording a particular event in which he or she is a participant.

[3.88] On the other hand, a number of arguments have been made against participant monitoring:

- one of the purposes of surveillance devices legislation is to offer protection to individuals, including protection of their privacy—permitting the recording of a private conversation or activity without the knowledge or consent of those

---

312 Additionally, there is a 'similarity of function' between taking notes and recording a conversation and this is an 'important reason for not prohibiting participant monitoring'. See ALRC Report No 22 (1983) vol 2, [1133]; and NSWLRC Interim Report No 98 (2001) app A, [A5], [A7]–[A8] and at [2.101] in which it was stated that:

> The major argument in favour of participant monitoring is that, as a party to a conversation or activity, a person has an express or implied right to hear the words spoken during that conversation or view the activity. The argument follows that the right to record the conversation or activity flows from the right to observe and be a party to it, and is no more intrusive on privacy than if the person took written notes.

313 NSWLRC Interim Report No 98 (2001) app A, [A10].

recorded would undermine that purpose, and would be inconsistent with a general expectation that monitoring will not occur without consent;[314]

- participant monitoring is no more acceptable than covert surveillance by a third party, and is no less severe a breach of privacy—whether participant monitoring is justified should be determined according to the circumstances, rather than whether the person conducting the monitoring was a party;[315]
- participant monitoring may have a 'chilling effect' that discourages people from speaking freely or participating in some activities;[316]
- participant monitoring is not equivalent to note taking and requires greater control, particularly because the latter cannot be done covertly, is less compelling and accurate, and has less potential for distribution;[317]
- permitting participant monitoring but restricting the disclosure of information obtained may be insufficient because:[318]
  - a recording remains vulnerable to use or dissemination;
  - the exceptions under which publication or communication may be permitted are broad; and
  - surveillance itself may cause harm to a person, for example, stress and emotional harm, insecurity and loss of trust, and a 'desensitisation to surveillance, leading to a narrowing of people's reasonable expectations of privacy'; and
- participant monitoring places the monitoring party at an unfair advantage because they can modify and control their behaviour based upon the knowledge that the conversation is being recorded.[319]

[3.89] In this context, it has been said that:[320]

---

314 ALRC Report No 123 (2014) [14.49]; NSWLRC Interim Report No 98 (2001) [2.102], [2.104]; VLRC Report No 18 (2010) [6.75]. See also ALRC Report No 22 (1983) vol 2, [1134], in which it was noted that the law has a place 'in upholding the right of the individual to control, to an appropriate extent, the "information penumbra" about him'.

315 NSWLRC Interim Report No 98 (2001) [2.105], [6.32]. More generally, the ALRC observed that a general provision for participant monitoring would permit surveillance even when it was not justifiable in the circumstances: ALRC Report No 123 (2014) [14.57].

316 ALRC Report No 123 (2014) [14.49]; ALRC Report No 22 (1983) vol 2, [1134]. The ALRC notes in its 2014 report that this is an 'increasing risk', because of the readily-available technologies that allow surreptitious recording.

317 NSWLRC Interim Report No 98 (2001) [2.105].

318 VLRC Consultation Paper No 7 (2009) [6.135]; ALRC Report No 123 (2014) [14.55], citing NZLC Report No 113 (2010) [2.5]; NZLC Issues Paper No 14 (2009) [8.62]–[8.73]. See also ACT Review (2016) [6.10].

319 ALRC Report No 22 (1983) [1128], [1134]. A person may also be empowered because they might present matters in a way that is favourable to their position because they have control of the situation, or because other parties may have less opportunity to dispute, qualify or contextualise the conversation.

320 VLRC Report No 18 (2010) [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. 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. (note omitted)

[3.90] Most other law reform reviews and inquiries that have considered participant monitoring have concluded that its use should be limited, with many suggesting that it be permitted (by exception) only in specific circumstances in which it is considered justified.[321] For example, the NZLC observed generally that:[322]

> it is clear that there are circumstances in which participant monitoring has a legitimate purpose and function in protecting both private and public interests. There are occasions when important public interests are served by permitting the parties and authorised outsiders to record and monitor private communications. Examples include investigative reporting by the media, members of the public protecting their own legal positions, and investigations by law enforcement agencies. (note omitted)

[3.91] It has been observed in this regard that specific exceptions 'are better able to protect the interests of participants',[323] but that '[a]ny 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'.[324]

[3.92] Some have suggested exceptions to permit participant monitoring where it is in the public interest or to protect a person's lawful interests.[325]

[3.93] For example, the NZLC stated that 'public interest' and 'lawful interests' exceptions should be included in a broad statement of the purposes for which participating monitoring may be undertaken. It explained that:[326]

> The breadth of these formulations likely renders most participant recordings lawful, and the adoption of such broad limits may not represent a major limitation on the participant monitoring exception. That being said, these broad formulations may be of value in clarifying that participant recordings made without justification are not defensible.

[3.94] The NZLC viewed these purposes broadly, and considered that the 'lawful interests' exception would be wide enough to encompass recording by a journalist to

---

321 ALRC Report No 123 (2014) [14.56]–[14.57]; VLRC Report No 18 (2010) [6.59] ff; ACT Review (2016) [6.10]; NSWLRC Interim Report No 98 (2001) [2.107]; NZLC Report No 113 (2010) [3.80]. See also ALRC Report No 22 (1983) vol 2, [1134].

322 NZLC Report No 113 (2010) [3.80].

323 ACT Review (2016) [6.10].

324 VLRC Report No 18 (2010) [6.76].

325 See, eg, ALRC Report No 123 (2014) [14.57]; VLRC Report No 18 (2010) [6.59] ff; ACT Review (2016) [6.10].

326 NZLC Report No 113 (2010) [3.84], [3.86].

ensure an accurate account of an interview, or a recording by a party to a conversation where it is important to keep an accurate record.[327]

[3.95] Others, however, have expressed concern about the breadth or uncertainty of such exceptions, including that they are open to misinterpretation or abuse and that the meaning of some terms (for example, 'lawful interests') is unclear.[328]

[3.96] For example, in South Australia, general exceptions relating to the public interest or the protection of lawful interests were considered 'too broad and ill-defined' and 'unsuited to the threats to personal privacy posed by the technological realities of the 21st century'. Legislation in that State was redrafted to include 'more specific and targeted allowances … for lawful use [of surveillance devices]'.[329]

[3.97] As an alternative, the NSWLRC suggested that legislation should focus on the circumstances in which recording without the knowledge or consent of others should be permitted, stating that it 'should not distinguish between monitoring conducted by parties and non-parties, but should facilitate covert surveillance when it can be justified in any particular situation'.[330]

Preliminary view

[3.98] The Commission considers that the proposed legislative framework in Queensland should not include a general exception for participant monitoring.

[3.99] This approach is consistent with the surveillance devices legislation in several other jurisdictions, and with Commonwealth law regulating telecommunications. It is also consistent with the position taken in other law reform reviews and inquiries that have considered this issue.[331]

[3.100] Since the introduction of the *Invasion of Privacy Act 1971*, there have been significant technological advances relevant to surveillance. For example, an audio or visual recording device may now be much smaller, can be built into other technology such as a mobile phone, and may have much greater recording capability. Additionally, a surveillance device of this kind is easily accessible to members of the public. As a result, there is now greater scope for an individual to be able to engage in covert recording or participant monitoring.

[3.101] The *Invasion of Privacy Act 1971*—which applies only to a listening device and permits participant monitoring—now offers insufficient regulation and protection of privacy. Permitting an individual to engage in participant monitoring, in circumstances where a surveillance device is easily accessible and a recording can

---

327 Ibid [3.87].

328 See, eg, NSWLRC Interim Report No 98 (2001) [2.102], [2.104]; ALRC Report No 22 (1983) vol 2, [1135].

329 South Australia, *Parliamentary Debates*, House of Assembly, 10 September 2015, 2476 (JR Rau, Deputy Premier, Attorney-General, Minister for Justice Reform, Minister for Planning, Minister for Housing and Urban Development, Minister for Industrial Relations and Minister for Child Protection Reform).

330 NSWLRC Interim Report No 98 (2001) [2.107].

331 These bodies include the ALRC, NSWLRC and VLRC.

be quickly, easily and widely disseminated, is a significant intrusion into individual privacy.

[3.102] The Commission considers that, in order to adequately protect privacy, participant monitoring should generally be prohibited under surveillance devices legislation. This is a significant change in policy, but is necessary in light of these significant technological advances.

[3.103] In limited circumstances, it may be appropriate for a person to record a conversation to which they are a party without the knowledge or consent of other participants. These might include, for example, a person who is being threatened or experiencing domestic violence.

[3.104] The Commission considers that these circumstances are more appropriately addressed by including specific exceptions in legislation. This approach achieves a balance between the need to protect individual privacy in the context of civil surveillance technologies, and the need for a person to be able to covertly record another in limited, exceptional circumstances.

[3.105] A number of relevant exceptions, such as a person's lawful interests, the public interest, or considerations of safety and well-being are discussed below.

Use of a surveillance device in a person's lawful interests

[3.106] In those jurisdictions that do not generally permit participant monitoring, a party to a private conversation or activity may use a listening device or optical surveillance device to record that conversation or activity if it is reasonably necessary for the protection of their lawful interests.[332] Where this exception applies, a party is permitted to record a conversation or activity without the knowledge or consent of the other parties.

[3.107] In jurisdictions where the term 'party' includes both principal parties and others who are listening or recording with consent, the surveillance devices legislation generally provides that a party may record with the consent of 'a principal party' if it is reasonably necessary to protect that principal party's lawful interests.[333] In effect, a recording may be made by a principal party without the knowledge or consent of others (that is, the principal party 'consents' to making the recording themselves to protect their own lawful interests), or by a party with the knowledge and consent of one principal party.

[3.108] For example, if A and B are having a private conversation they are both principal parties. If A considers that it is in his or her lawful interests, A may record the conversation without the knowledge or consent of B. If C is permitted to listen to

---

332 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Surveillance Devices Act 2016* (SA) s 4(2)(a)(ii); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii). In the Australian Capital Territory and Western Australia, a person may also use a device on behalf of a party in these circumstances.

333 *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(d), 6(3)(b)(iii). In the Australian Capital Territory, the recording must be considered by the consenting principal party, on reasonable grounds, to be necessary for the protection of that principal party's lawful interests. As to 'party' and 'principal party', see [2.77]–[2.78] above. See also ALRC Report No 123 (2014) [14.53] as to the *Telecommunications (Interception and Access) Act 1979* (Cth).

that conversation, C could record the conversation with A's consent and to protect A's lawful interests without the knowledge or consent of B.

[3.109] In South Australia, a person may also install, use or maintain:[334]

- a listening device on or within premises or a vehicle, if an owner or occupier agrees and it is reasonably necessary for the protection of the lawful interests of the owner or occupier or some other person; or
- an optical surveillance device on premises without fulfilling the requirement for consent,[335] if the use of the device is reasonably necessary to protect that person's lawful interests.

[3.110] The term 'lawful interests' is not defined by surveillance devices legislation, but has been the subject of judicial consideration.

[3.111] It has been described as referring to 'interests that are not unlawful', and as similar to a 'legitimate interest' or an interest that conforms to law. The term should be distinguished from 'legal interests' and, for a lawful interest to exist, it is not required that there be a legal right, title, duty or liability.[336]

[3.112] In *Thomas v Nash*, the Supreme Court of South Australia analysed cases that have considered the meaning of 'lawful interests' in the context of surveillance devices legislation:[337]

> In none of those decisions is there an attempt to identify comprehensively the scope of the expression 'lawful interests'. That is not surprising. It is an expression which is best left to be applied case by case, subject to some general guidelines.
>
> Each decision is an application of the expression to its particular facts. In most of those decisions it was accepted that a mere desire to have a reliable record of a conversation is not enough. I agree. Most of the decisions proceed on the basis that a desire to gain an advantage in civil proceedings would not ordinarily amount to a relevant lawful interest, although of course each case has to be considered on its facts. Several of the cases proceed on the basis that where the conversation relates to a serious crime, or an allegation of a serious crime, or to

334 *Surveillance Devices Act 2016* (SA) ss 4(2)(c), 5(4)(b). As to the definition of 'premises', see n 301 above.

335 A person who uses an optical surveillance device is required to obtain consent from the parties and the owner or occupier of the premises, vehicle or thing: *Surveillance Devices Act 2016* (SA) s 5(1)–(3). See [3.76]–[3.77] above.

336 *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, [27]–[33]; see also ACT Review (2016) [6.14]. Cf the Privacy Committee of South Australia, in response to questions on notice from the South Australian Legislative Review Committee, which considered that 'the protection of lawful interests is understood to mean the protection of an interest of an individual or body corporate that is established by law. It could be a financial or property interest arising from a contractual agreement, or other interest, right or claim established under law': see SA Legislative Review Committee Report (2013) 38; Privacy Committee of South Australia, *Responses to questions on notice from the South Australian Legislative Review Committee: Inquiry into surveillance devices* (2013) 2.

337 *Thomas v Nash* (2010) 107 SASR 309, [47]–[48]. Similarly, in *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580 it was stated, at [32], that a person may not have a lawful interest in recording every conversation to which they are a party, but may have a lawful interests in, for example, recording a conversation that was to result in an oral contract, a threatening phone call, or a conversation that is part of a blackmail attempt.

In the Australian Capital Territory, it was suggested that a person may consider the use of a listening device necessary to protect their lawful interests where they believe that they 'may be blackmailed in the course of a pending conversation': Explanatory Memorandum, Listening Devices Bill 1991 (ACT) 2.

> resisting such an allegation, a court is more likely to find that the recording of a conversation relating to the crime can be made in the protection of the person's "lawful interests".

[3.113] It has also been stated that there must be more than a potential for a recording to be used to the person's advantage in the future.[338]

[3.114] In *Sepulveda v The Queen*, the New South Wales Court of Criminal Appeal stated that the lawful interests exception 'should not be interpreted in such a way as to render otiose the primary purpose of the Act, which is to protect privacy by prohibiting covert recording of a conversation other than (usually) by way of a warrant under the Act'.[339] However, the need to establish the scope of 'lawful interests' is offset by the requirement that the use be 'reasonably necessary' to protect those interests. The question of reasonable necessity should be judged objectively and based upon the circumstances existing at the time of recording, taking into account:[340]

- the extent to which the recording was necessary to protect the relevant interests;
- other means available to address the matter or obtain a recording (for example, by reporting a crime to police); and
- whether the intrusion into privacy that occurs when a recording is made is justified, taking into account the interests that are being protected.

[3.115] It has been explained that, by applying this approach:[341]

> the courts have balanced the interest protected by the recording against the interests of privacy in the particular circumstances. In this way a flexible approach to the range of interests that might justify surveillance is balanced against the need for protection of that interest to be proportionate to the interference with privacy involved.

[3.116] The lawful interests exception has been discussed in several reviews and inquiries undertaken in other jurisdictions. In the ACT Review, it was recommended that any exception based on lawful interests 'requires an objective evaluation of the purposes for which surveillance or communication is carried out, and whether that surveillance or communication was necessary and proportionate'.[342]

---

338 *Thomas v Nash* (2010) 107 SASR 309, [45]; *Marsden v Amalgamated Television Services* [2000] NSWSC 465, [20]–[23].

339 *Sepulveda v The Queen* (2006) 167 A Crim R 108, [115], [142]; see also *Thomas v Nash* (2010) 107 SASR 309, [49]; ACT Review (2016) [6.14].

340 *Sepulveda v The Queen* (2006) 167 A Crim R 108, [116]–[118], [138]–[139], [142]; *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, [23], [32]; *Marsden v Amalgamated Television Services* [2000] NSWSC 465, [14], [17]-[18], [20]–[23]; *Georgiou Building Pty Ltd v Perrinepod Pty Ltd* (2012) 261 FLR 211. See also ACT Review (2016) [6.14]–[6.15]. It was also explained in *Georgiou* that the word 'necessary' should, in this context, be construed as meaning 'appropriate, but not essential or unavoidable': [16].

341 ACT Review (2016) [6.15].

342 Ibid [2.5](c).

[3.117] The South Australian Legislative Review Committee similarly concluded that what is a 'lawful interest' is a matter to be determined objectively in the particular circumstances at the time immediately before use of the surveillance device, and that those interests must be 'balanced against other interests, such as the interest in protecting personal privacy'.[343]

[3.118] The VLRC supported an exception for participant monitoring where it is to protect a person's lawful interests, but stated that the exception 'should not be too broad'. The VLRC explained that it did not favour a broad interpretation that would permit participant monitoring in order to keep an accurate record,[344] or an interpretation so narrow that it would exclude monitoring for evidentiary purposes.[345]

[3.119] Conversely, it has been observed that the meaning of the term 'lawful interests' is uncertain, and that exceptions to participant monitoring are potentially very broad.[346] There has been some suggestion that including lawful interests as an exception is not a 'sufficient check' on the power to engage in participant monitoring, and that a court should determine whether covert recording is necessary to protect a person's lawful interests.[347]

Use of a surveillance device in the public interest

[3.120] In some jurisdictions, legislation includes an exception for the use of a listening device or optical surveillance device in the 'public interest'. These provisions may permit a party to engage in participant monitoring, or another person to use a surveillance device to listen to, observe or record a conversation or activity.

[3.121] Such an exception may be relevant to the use of a surveillance device by a media organisation, journalist or private investigator.

[3.122] In Western Australia and the Northern Territory, the term 'public interest' is defined by surveillance devices legislation to include:[348]

> the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens.

[3.123] In these jurisdictions, exceptions relevant to the public interest do not apply if, in the course of installing or using a device, a person does an unlawful act.[349]

---

343 SA Legislative Review Committee Report (2013) 38, which considered the Surveillance Devices Bill 2012 (SA) (not passed).

344 This was proposed by the NZLC: see [3.93]–[3.94] above.

345 VLRC Report No 18 (2010) [6.78]–[6.79].

346 See, eg, NSWLRC Interim Report No 98 (2001) [2.102], [2.104]; ALRC Report No 22 (1983) vol 2, [1130], [1135]. See also [3.95]–[3.97] above.

347 NSWLRC Interim Report No 98 (2001) [2.102], note 149. The NSWLRC recommended that covert surveillance should be permitted when justified in the circumstances, and should not be dependent on whether or not a person is a party. Generally, the NSWLRC recommended a scheme in which a person who wants to use covert surveillance should be required to obtain prior authorisation. See [3.97] above, [D.7]–[D.8] below.

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

349 *Surveillance Devices Act* (NT) s 42; *Surveillance Devices Act 1998* (WA) s 25. Specifically, the legislation refers to an act that is unlawful under any law except the surveillance devices legislation in that jurisdiction.

These provisions permit the use of a listening device or optical surveillance device to record, monitor, listen to or observe (or similar) a private conversation or activity:

- by a party or a person acting on their behalf, if there are reasonable grounds for believing that the use of the device is in the public interest;[350]
- by a person on behalf of a child or protected person under their care or supervision who is a principal party, if there are reasonable grounds for believing that the use of the device will contribute toward the protection of their best interests and is in the public interest;[351]
- by a person if at the time of use there are 'reasonable grounds for believing that the circumstances are so serious and the matter is of such urgency' that the use of the device is in the public interest (an 'emergency use').[352]

[3.124] In Western Australia, it was explained that the approach was intended to have only 'minimal impact' on the media, private investigators and the public on the 'rare occasions' where covert surveillance was carried out in the public interest. It was stated that this approach:[353]

> maintains the privacy rights of the individual by allowing surveillance only when there is a strong public interest in doing so. A principal party to the private conversation or activity must usually consent to the surveillance, unless the matter is so serious and urgent that it is in the public interest to use the device even without the consent of a principal party. If surveillance is carried out without the consent of a principal party, a written report must be delivered to a judge explaining that the surveillance occurred. The judge has a discretion to destroy the recording if it was not made in the public interest. [It] therefore maintains the protection of the individual's right to privacy. Furthermore, the part does not apply if the surveillance is connected with an unlawful act, such as trespass.

[3.125] In South Australia, the prohibitions against using a listening device or optical surveillance device to listen to, observe, monitor or record a private conversation or private activity do not apply if the use of the device is in the public interest.[354] The term 'public interest' is not defined in South Australia.

[3.126] In response to questions on notice from the South Australian Legislative Review Committee and in the context of that Committee's inquiry into surveillance devices, the Privacy Committee of South Australia noted the importance of distinguishing between matters that are 'genuinely in the public interest' and those

---

350 *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(1), (2), 27(1), (2). A recording may be made by a principal party without the knowledge of others, or by another party with the consent of one principal party.

351 *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3).

352 *Surveillance Devices Act* (NT) ss 11(2)(c), 12(2)(e), 43, 44; *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 28, 29. These provisions also include procedures for reporting the emergency use to a judge: *Surveillance Devices Act* (NT) s 45; *Surveillance Devices Act 1998* (WA) s 30.

353 Western Australia, *Parliamentary Debates*, Legislative Council, 21 October 1998, 2406 (NF Moore, Leader of the House).

354 *Surveillance Devices Act 2016* (SA) s 6(1)(a), 2(a). More specifically, the prohibitions also do not apply to the installation, use or maintenance of a listening device or optical surveillance device under the provisions about investigation agents and loss adjusters, or of an optical surveillance device on premises where it is reasonably necessary to protect a person's lawful interests, if the use of the device is in the public interest: s 6(1)(b), 2(b). See also [3.106] ff above, [3.145] ff below.

that 'are merely of interest to the public'.[355] They explained that what is in the public interest depends upon the context and circumstances and that:[356]

> *public interest* is generally considered to be something of public importance or something that will benefit the public rather than the private interests of an individual. … [I]n some cases an individual interest could also represent a broader *public interest* where its general application would result in a broader interest to the public. (emphasis in original)

[3.127] A public interest exception was supported in the ACT Review, noting that the concept is generally interpreted broadly.[357] It was recommended that legislation 'allow surveillance when it is carried out to protect a public interest and the surveillance activity is necessary and proportionate'.[358]

[3.128] The VLRC did not recommend a 'broad public interest exception' as the scope would be 'too uncertain for use in a regime that contains criminal sanctions'.[359]

[3.129] The ALRC and NSWLRC proposed alternative legislative schemes.

[3.130] The NSWLRC proposed that covert surveillance should be permitted in the public interest only where it is authorised by an 'appropriate issuing authority',[360] having regard to factors such as:[361]

- the nature of the issue in respect of which the authorisation is sought;
- the public interest (or interests) arising from the circumstances;
- the extent to which the privacy of any person is likely to be affected;
- whether measures other than covert surveillance have been used or may be more effective;
- the intended use of any information obtained as a result;

---

355 SA Legislative Review Committee Report (2013) 38; Privacy Committee of South Australia, *Responses to questions on notice from the South Australian Legislative Review Committee: Inquiry into surveillance devices* (2013) 2. See also ACT Review (2016) [6.18]. In South Australia, covert recordings of a suspect by a police informant have been found to be in the public interest: See, eg, *R v Giaccio* (1997) 68 SASR 484; *R v Smith* (1994) 63 SASR 123; see also SA Legislative Review Committee Report (2013) 38.

356 SA Legislative Review Committee Report (2013) 38; Privacy Committee of South Australia, *Responses to questions on notice from the South Australian Legislative Review Committee: Inquiry into surveillance devices* (2013) 2. See also ACT Review (2016) [6.18].

357 ACT Review (2016) [6.21]. This review explained the meaning of the term 'public interest' in a similar way to the Privacy Committee of South Australia.

358 ACT Review (2016) [2.5](d), [6.21]. However, it was also recommended that subsequent communication should be subject to additional regulation: see [3.185] ff, [3.198] below.

359 VLRC Report No 18 (2010) [6.81].

360 It was proposed that the 'issuing authority' could be members of a court or tribunal, and more generally that it should be 'accessible, affordable, expeditious and impartial': NSWLRC Interim Report No 98 (2001) [6.34]-[3.36], Rec 52.

361 NSWLRC Interim Report No 98 (2001) [6.37]–[3.38], Rec 54; NSWLRC Report No 108 (2005) [5.47], Rec 3. The NSWLRC also considered that any authorisation issued should specify a number of matters, including the circumstances in respect of which it is granted and the various public interests that were considered: NSWLRC Interim Report No 98 (2001) [6.39]–[6.42], Rec 55.

- the role played by the media in upholding the public interest; and
- whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.

[3.131] It was recommended that the scheme apply to any person (except an employer or law enforcement officer), including a journalist, media organisation or private investigator. Additionally, the term 'public interest' was to be interpreted broadly, noting that it 'may include private rights and interests where appropriate'.[362]

[3.132] The NSWLRC expressed concern that a broader exception permitting surveillance in the public interest would be open to abuse, unable to appropriately limit unwarranted intrusions into privacy and have the result that only a law enforcement officer or employer would be subject to authorisation requirements.[363]

[3.133] The ALRC observed that a broad public interest defence might allow for the wider use of surveillance based upon subjective views, and instead proposed a defence of 'responsible journalism'. The ALRC stated:[364]

> Media and journalistic activities offer significant public benefit, and these activities may at times justify the use of surveillance devices without the notice or consent of the individuals placed under surveillance.
>
> …
>
> At the same time … a defence of responsible journalism should be suitably constrained. The defence should not, for example, allow unrestricted freedom to carry out surveillance in circumstances which are not journalistic in nature, where the public interest in a matter is trivial, or where the matter is merely of interest to the public or for the purposes of gossip.

[3.134] In relation to installing or using a device, the defence should depend on 'whether it was reasonable for the journalist to believe that the use of the surveillance device was in the public interest', and not on whether the information obtained is in the public interest. Generally, elements of the defence might include:[365]

- the surveillance should be carried out for the purposes of investigating matters of significant public concern, such as corruption;
- the defendant must have reasonably believed that conducting the surveillance was in the public interest;
- the surveillance was necessary and appropriate for achieving that public interest, and the public interest could not have been satisfied through other reasonable means; and

---

362 NSWLRC Interim Report No 98 (2001) Recs 49, 50. The NSWLRC concluded in its final report that this authorisation scheme was appropriate and that, despite strong opposition, it should apply to the media: NSWLRC Report No 108 (2005) [5.46]; [5.24]–[5.49]. See also [3.194]–[3.196] below.

363 NSWLRC Interim Report No 98 (2001) [6.24]–[6.27].

364 ALRC Report No 123 (2014) [14.58] ff. The ALRC stated that this defence is particularly important if participant monitoring exceptions are not included in legislation.

365 ALRC Report No 123 (2014) [14.62]–[14.64]. The ALRC considered that there should be separate provision for the use or installation of a surveillance device, and for the communication of information obtained through surveillance. As to communication, see [3.197] below.

- the defendant must have been an employee or member of an organisation that had publicly committed to observing standards dealing adequately with the appropriate use of surveillance devices by media and journalists. (notes omitted)

Use of a surveillance device for safety and well-being

[3.135] In two jurisdictions—Western Australia and Tasmania—a person is generally permitted to listen to or record a conversation or activity if it is for a purpose connected with ensuring safety or well-being. This exception permits participant monitoring by or on behalf of a party, and in some instances permits the use of a device by any person.

[3.136] In Western Australia, where a child or a 'protected person'[366] is a principal party to a private conversation or activity, another person responsible for their care, supervision or authority may use a listening device or optical surveillance device on their behalf. There must be reasonable grounds for believing that the use of the device will contribute to the protection of the child's or protected person's best interests and is in the public interest.[367]

[3.137] In Tasmania, a person is permitted to use a listening device to obtain evidence or information connected with an imminent threat of serious violence or substantial property damage, or a serious narcotics offence. The person must believe on reasonable grounds that it was necessary to use the device immediately to obtain the evidence or information.[368] This exception 'is designed to cover gravely serious situations such as the taking of hostages, bombing threats and serious drug offences' where use of the device is immediately necessary, and is included 'to enable law enforcement agencies to act quickly and effectively'.[369]

Use of a surveillance device that is not for communication or publication

[3.138] In some jurisdictions, a party to a private conversation is not prohibited from recording that conversation if it is with the consent of a principal party and not for the

366 A 'protected person' is a person who has a mental impairment and is therefore unable to consent to the use of a listening device or optical surveillance device in accordance with the public interest provisions: *Surveillance Devices Act 1998* (WA) ss 26(4), 27(4). These provisions do not apply if, in the course of installing or using a device, an act is done that is unlawful under any law or any Act other than the *Surveillance Devices Act 1998* (WA): s 25.

367 *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3).

368 *Listening Devices Act 1991* (Tas) s 5(2)(c). A 'serious narcotics offence' is defined as an offence under the *Misuse of Drugs Act 2001* (Tas), unless declared otherwise by regulation: s 3(1). Where this exception is relied upon, the user is required to provide reports about (among other things) the circumstances and particulars of the use of the device to the Chief Magistrate and the Attorney General. In some circumstances, the Chief Magistrate may make particular orders following the receipt of a report, for example, that an ongoing use of a device be ceased or that a person be informed of the use of the device: ss 5(4)–(7), 6–8.

See also, in relation to a law enforcement officer only, the *Surveillance Devices Act* (NT) s 11(2)(b); *Surveillance Devices Act 1999* (Vic) s 6(2)(c).

369 Tasmania, *Parliamentary Debates*, Legislative Assembly (1 May 1991) 934–5 (PJ Patmore, Minister for Justice).

purpose of communicating or publishing the conversation, or a report of the conversation, to a person who is not a party to that conversation.[370]

[3.139] The VLRC commented that it did not recommend this exception because 'it is still possible that recordings made by a party to a conversation or activity may fall into the hands of third parties'.[371]

Use of a surveillance device for a lawful purpose

[3.140] In New South Wales, a person is not prohibited from using a tracking device to determine the geographical location of a person or object 'for a lawful purpose'.[372]

[3.141] The term 'lawful purpose' is not defined. The VLRC criticised this exception as being 'vague and unnecessarily broad', and suggested that there are other ways to ensure relevant interests are taken into account when determining whether tracking technology should be used. It was suggested that specific law enforcement activities could be exempted by regulation, which should ensure appropriate oversight of the decision (including consultation and parliamentary scrutiny).[373]

Use of a surveillance device by a private investigator or loss adjuster

[3.142] In Queensland, there is no specific exception for the use of a listening device by a private investigator. A private investigator must be licensed under the *Security Providers Act 1993*.[374] A private investigator is a person who, for a reward:[375]

- obtains and gives private information about another person, without the other person's express consent; or
- carries out surveillance for obtaining private information[376] about another person, without the other person's express consent; or

---

370 *Listening Devices Act 1992* (ACT) s 4(3)(b)(ii); *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(ii); *Listening Devices Act 1991* (Tas) s 5(3)(b)(ii).

371 VLRC Report No 18 (2010) [6.81].

372 *Surveillance Devices Act 2007* (NSW) s 9(2)(c).

373 VLRC Report No 18 (2010) [6.42] ff. The VLRC suggested that this exception might have been relied upon by the New South Wales government to enable the use of ANPR technology as part of the Safe-T-Cam traffic monitoring system.

374 See generally *Security Providers Act 1993* (Qld) pt 2. To become licensed an individual must be 18 years or older, must be an 'appropriate person' and is required to complete an appropriate training course. In determining whether a person is an 'appropriate person', relevant considerations include whether the person has shown dishonesty or lack of integrity or used harassing tactics in dealings in which they were involved, been bankrupt or been convicted of particular offences, and any other information indicating that the person is a risk to public safety or that it would be contrary to the public interest for the person to hold a licence: s 11(2)–(5).

375 *Security Providers Act 1993* (Qld) s 6(1). See also: Institute of Mercantile Agents, *Investigators* <http://www.imal.com.au/index.php?option=com_content&view=article&id=34:queensland&catid=25:states-a-territory-info>; Queensland Government, *Apply for a Private Investigator Licence* (10 October 2018) <https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/regulated-industries-licensing-and-legislation/security-industry-regulation/get-a-security-licence/security-manpower-licence/apply-for-a-private-investigator-licence>.

376 For an individual, 'private information' refers to information about their personal character, actions, business or occupation. For a person other than an individual, 'private information' relates to the person's business or occupation. The reference to 'information' includes information that is recorded in a document: *Security Providers Act 1993* (Qld) s 6(5) (definition of 'private information').

- investigates the disappearance of a missing person.

[3.143] However, a person is not a private investigator (and does not require a licence) if they are an Australian legal practitioner, an accountant, or a person carrying on the business of insurance or an insurance adjustment agency and they are performing the functions of their occupation.[377]

[3.144] Other people must also be licensed under the *Security Providers Act 1993*. These include, for example, a crowd controller[378] and a security officer.[379] A security officer may, for a reward and among other things, monitor another person's property 'by operating an audiovisual or visual recording system, a radio or other electronic monitoring device'.[380]

[3.145] In South Australia, a licensed investigation agent[381] or a loss adjuster[382] is not prohibited from using a listening device or optical surveillance device if the use is part of performing their role and is reasonably necessary to protect a person's lawful interests,[383] or if the use is in the public interest.[384]

[3.146] The South Australian Legislative Review Committee and the NSWLRC observed that an investigation agent or a private investigator would primarily use covert surveillance to detect insurance fraud. The Committee, recognising the potential impact on an individual, recommended that there should be 'greater parity' with the requirements for a law enforcement officer, so that an investigator acting on behalf of an insurer may only use covert surveillance in the public interest or to protect a person's lawful interests and with authorisation.[385] The NSWLRC stated

---

377 *Security Providers Act 1993* (Qld) s 6(3). In each instance, this also includes an employee of that person.

378 A 'crowd controller' is described as a person who is at a public place principally to keep order, including by monitoring or controlling the behaviour of people in the place. An example of a crowd controller is a bouncer at a hotel: *Security Providers Act 1993* (Qld) s 5(1).

379 Other people who must have a licence are bodyguards, security advisers, security equipment installers and security firms: *Security Providers Act 1993* (Qld) pt 1. 'Security equipment' includes electronic equipment that is designed to protect or watch property, for example, an audio or visual recording system, an access control device (including a biometric access control device) and an intrusion detector (including motion, contact and infra-red detectors): s 8A.

380 *Security Providers Act 1993* (Qld) s 7(1).

381 That is, a person who holds an investigation agent's licence under the *Security and Investigation Industry Act 1995* (SA), which authorises the person to perform the functions of 'inquiry work': *Surveillance Devices Act 2016* (SA) s 4(2)(b)(iv). Inquiry work includes searching for information about a person's character, actions or their work and gathering evidence to be used in court: Government of South Australia, *Security and Investigation Agent Licence* (14 September 2018) <https://www.sa.gov.au/topics/business-and-trade/licensing/security/security-and-investigation-agent-licence>.

382 Specifically, a loss adjuster to whom the *Security and Investigation Industry Act 1995* (SA) does not apply: *Surveillance Devices Act 2016* (SA) s 4(2)(b)(v). Generally, a loss adjuster is an insurance agent who assesses the amount of compensation that should be paid following a loss: *Merriam-Webster Dictionary* (online, 2018) <https://www.merriam-webster.com/dictionary/loss%20adjuster>.

383 *Surveillance Devices Act 2016* (SA) ss 4(2)(b)(iv), (v), 5(4)(a)(iv), (v), (5).

384 *Surveillance Devices Act 2016* (SA) s 6(1)(b), (2)(b).

385 See the SA Legislative Review Committee Report (2013) 63–71, 76, Rec 6, which considered the Surveillance Devices Bill 2012 (SA) (not passed). The Committee also recommended development of an enforceable code of practice, to assist in determining the circumstances in which covert surveillance might be in the public interest or might protect a person's lawful interests, and that further consideration be given to the circumstances in which a private investigator should be able to undertake covert surveillance on behalf of a private individual: 76–7, Recs 7, 9.

that it would be impractical to regulate private investigators individually, and recommended that an insurer should be authorised to conduct covert surveillance and to contract that work out to an investigator. For other uses of covert surveillance, it was proposed that a private investigator should be required to obtain authorisation.[386]

[3.147] In the ACT Review, it was observed that, in that jurisdiction, a private investigator is not required to be licensed or subject to a robust regulatory regime, although they do have a legitimate role in legal and support services. It was concluded that, in the absence of regulation, an investigator should not be the subject of exemptions.[387]

Unintentional use of a surveillance device

[3.148] In some jurisdictions, a person does not commit an offence if they unintentionally hear a private conversation by means of a listening device[388] or if the use of an optical surveillance device results in the unintentional recording or observation of a private activity.[389] In Queensland, this exception is limited to the unintentional hearing of a private conversation by means of a telephone.[390]

[3.149] In some jurisdictions, in the context of use by law enforcement, the surveillance devices legislation provides generally that an inadvertent, unexpected or incidental use of some listening devices or optical surveillance devices is not an offence.[391]

[3.150] More generally, the legislation in most jurisdictions provides that an offence is committed where a person acts 'knowingly' or 'intentionally'. In those jurisdictions, an accidental or unintentional use may not constitute an offence.[392]

[3.151] In the ACT Review, it was observed in particular that the use of drones by individuals may result in the inadvertent observation of private activities, and

---

386 NSWLRC Report No 108 (2005) [5.62]–[5.69], Rec 7. The Commission also recommended that insurers and private investigators be required to comply with requirements concerning record keeping, reporting, document inspection and restrictions on the use of surveillance material: see generally [5.50] ff.

Surveillance is conducted by private investigators for many purposes, including 'in areas ranging from workers' compensation and motor vehicle injury claims, to arson, intellectual property matters, family law, defamation, criminal matters, debt collection, repossession and process serving': NSWLRC, Interim Report No 98 (2001) [6.21].

387 ACT Review (2016) [2.5](h), [6.34]–[6.38].

388 *Listening Devices Act 1992* (ACT) s 4(2)(b); *Surveillance Devices Act 2007* (NSW) s 7(2)(c); *Surveillance Devices Act 2016* (SA) s 4(2)(f); *Listening Devices Act 1991* (Tas) s 5(2)(d); *Surveillance Devices Act 1998* (WA) s 5(2)(e).

389 *Surveillance Devices Act 1998* (WA) s 6(2)(e).

390 *Invasion of Privacy Act 1971* (Qld) s 43(2)(b).

391 *Surveillance Devices Act 2007* (NSW) s 50A; *Surveillance Devices Act* (NT) s 14A(3); *Surveillance Devices Act 1999* (Vic) ss 6(2)(d)–(e), 7(2)(d)–(e). This legislation is specific to body-worn devices used lawfully, which generally requires that their use is overt and in the course of the officer's duty.

392 See [3.58]–[3.62] above.

concluded that a prohibition on surveillance should exclude inadvertent observation.[393]

Location and retrieval of a surveillance device

[3.152] In some jurisdictions, a person does not commit an offence by using a device solely for the purpose of locating and retrieving that device.[394]

Use of a surveillance device in other prescribed circumstances

[3.153] In several jurisdictions, the surveillance devices legislation provides that it is not an offence to install, use, maintain or attach a device in 'prescribed circumstances'. In South Australia, circumstances may be prescribed in relation to any of the four categories of surveillance device,[395] but in the Northern Territory and Western Australia this is limited to a tracking device.[396]

[3.154] In relation to a tracking device, prescribed circumstances include:[397]

- to search for a person or thing during a search and rescue operation;
- to monitor the location of a hospital or nursing home patient in particular circumstances, for example, if a patient is legally obliged to stay but is likely to attempt to leave, or to locate a vulnerable patient if they become lost or go missing;
- to monitor the activities and location of an accused person, offender or prisoner, or to locate a prisoner if they escape from legal custody;
- to monitor the location of an animal or thing the subject of a research project;
- to measure transport system performance or monitor traffic; or
- to track an object that is believed to have been stolen.

---

393 ACT Review (2016) [2.5](f), [6.29]. However, it was also observed that 'communication or publication of the results of inadvertent observation … should be regulated through requiring a court order or as otherwise required by the public interest'.

394 *Surveillance Devices Act 2007* (NSW) ss 7(2)(e), 8(2)(c); *Surveillance Devices Act 2016* (SA) ss 4(2)(g), 5(4)(e), 7(2)(b). In New South Wales, this applies specifically in relation to listening devices and optical surveillance devices but also includes 'enhancement equipment' related to those devices, which is defined as equipment capable of enhancing a signal, image or other information obtained by the use of a surveillance device: s 4(1). In South Australia, it applies to listening devices, optical surveillance devices and tracking devices.

In the Australian Capital Territory, a person who used the 'find my iPad' service to locate a stolen iPad, including by identifying the vicinity of the iPad's location and by setting off an audio alarm to pinpoint the exact location, was found not to have physically or electronically trespassed on premises: B Arnold, 'Cloudy weather: privacy, media and new technologies' (2012) 9(2) *Privacy Law Bulletin* 20, 22.

395 *Surveillance Devices Act 2016* (SA) ss 4(2)(h), 5(4)(f), 7(2)(c), 8(2)(b). No circumstances have been prescribed in relation to listening devices, optical surveillance devices or data surveillance devices.

396 *Surveillance Devices Act* (NT) s 13(2)(d); *Surveillance Devices Act 1998* (WA) s 7(2)(d).

397 *Surveillance Devices Regulations* (NT) reg 3(1); *Surveillance Devices Regulations 2017* (SA) reg 11; *Surveillance Devices Regulations 1999* (WA) reg 6(1), (2).

Questions

A prohibition on the use of a surveillance device for particular purposes

Q-6 For what purposes should the use of a surveillance device be prohibited? For example, some or all of:

- **(a) overhearing, recording, monitoring or listening to a relevant conversation;**
- **(b) observing, monitoring or recording visually a relevant activity;**
- **(c) accessing, tracking, monitoring or recording information that is input into, output from or stored in a computer;**
- **(d) determining the geographical location of a person, vehicle or object;**
- **(e) some other purpose; for example, the collection of biometric data?**

Q-7 Should the prohibition in Q-6:

- **(a) be restricted to intentional or knowing use?**
- **(b) be restricted to private conversations and private activities, or should it extend to some other conversations and activities?**
- **(c) extend to attachment, installation or maintenance of the device?**

Exceptions to the prohibition on the use of a surveillance device

Q-8 In what circumstances should a person be permitted to use a surveillance device with consent? What should be the requirements of consent, and should this vary depending upon the particular use or type of device?

Q-9 Should there be a general exception to the prohibition in Q-6 to permit participant monitoring? Why or why not?

Q-10 If 'no' to Q-9, should there be any exceptions that permit participant monitoring in particular circumstances?

Q-11 If 'yes' to Q-10, what should be the particular circumstances for any exceptions and why? For example:

- **(a) to protect a person's lawful interests;**
- **(b) where it is in the public interest;**

(c) where it is consistent with a person's safety or well-being (for example, where there is an imminent threat of violence or property damage, or to protect a child or adult with impaired capacity); or

(d) where it is not intended to communicate or publish to a person who is not a party?

Q-12 Apart from participant monitoring, should there be any exceptions that permit a person to use a surveillance device without consent in particular circumstances?

Q-13 If 'yes' to Q-12, what should be the particular circumstances for any exceptions and why? For example:

(a) to protect a person's lawful interests;

(b) where it is in the public interest; or

(c) where it is consistent with a person's safety or well-being (for example, where there is an imminent threat of violence or property damage, or to protect a child or adult with impaired capacity)?

Q-14 Should there be other circumstances in which the use of a surveillance device is permitted or is not an offence, for example:

(a) for a lawful purpose;

(b) for certain people acting in the course of their occupation, such as media organisations, journalists, private investigators or loss adjusters;

(c) to locate or retrieve a device;

(d) where the use is unintentional; or

(e) in other prescribed circumstances?

If so, what provision should be made for these circumstances, and why?

Communication or publication of information obtained from a surveillance device

[3.155] Surveillance devices legislation generally prohibits the communication or publication of information obtained from the use of a surveillance device (the 'communication or publication prohibitions'), except in certain circumstances.[398]

[3.156] The provisions apply to information obtained from either the unlawful use or, except in New South Wales, the lawful use of a surveillance device. Their purpose is to prevent or limit the damage that could be caused by the communication or publication of information obtained in this way without consent.[399]

[3.157] They also set out a number of exceptions that permit a communication or publication, without consent, in particular circumstances in which the intrusion on privacy is justifiable. This may, for example, include use by an individual to protect their lawful interests, or by an investigative journalist in the public interest.

Queensland

[3.158] In Queensland, the *Invasion of Privacy Act 1971* contains two offence provisions prohibiting communication or publication, each with its own exceptions.

Communication or publication of a private conversation unlawfully listened to

[3.159] First, section 44(1) of the Act provides that it is an offence for a *person* to communicate or publish to another person a private conversation, or a report of, or of the substance, meaning or purport of, a private conversation that has come to their knowledge as a result, directly or indirectly, of the unlawful use of a listening device.

[3.160] This offence does not apply:[400]

- if the communication or publication is made:
  - to a party to the conversation or with the consent, express or implied, of such a party; or
  - in the course of proceedings for an offence against part 4 of the Act; or
- to prevent a person from communicating or publishing knowledge of a private conversation that was not obtained through the unlawful use of a listening device, even if that person also obtained knowledge of the conversation through the unlawful use of a listening device.

---

398 *Listening Devices Act 1992* (ACT) ss 5, 6; *Surveillance Devices Act 2007* (NSW) ss 11, 14; *Surveillance Devices Act* (NT) s 15; *Invasion of Privacy Act 1971* (Qld) ss 44, 45; *Surveillance Devices Act 2016* (SA) ss 9, 10, 12; *Listening Devices Act 1991* (Tas) ss 9, 10; *Surveillance Devices Act 1999* (Vic) s 11; *Surveillance Devices Act 1998* (WA) s 9.

399 See, eg, Australian Capital Territory, *Parliamentary Debates*, Legislative Assembly, 20 August 1992, 1879–80; Tasmania, *Parliamentary Debates*, Legislative Assembly, 1 May 1991, 935; Victoria, *Parliamentary Debates*, Legislative Council, 5 May 1999, 424.

400 *Invasion of Privacy Act 1971* (Qld) s 44(2).

Communication or publication of a private conversation by a party

[3.161] Second, section 45(1) of the Act provides that it is an offence for a *party* to a private conversation who used a listening device to overhear, record, monitor or listen to that conversation, to subsequently communicate or publish to another person any record of the conversation made, directly or indirectly, by the use of the listening device.[401]

[3.162] This offence does not apply where the communication or publication is:[402]

- made to another party to the private conversation;
- made with the express or implied consent of all other parties to the private conversation who were speaking or spoken to during the conversation;
- made in the course of legal proceedings;
- not more than is reasonably necessary:
  - in the public interest; or
  - in the performance of a duty of the person making the communication or publication; or
  - for the protection of that person's lawful interests;
- made to a person who has, or is believed on reasonable grounds to have, such an interest in the private conversation as to make the communication or publication reasonable under the circumstances in which it is made; or
- in general terms, made by a person who used the listening device in connection with law enforcement.

Other jurisdictions

[3.163] The surveillance devices legislation in the Australian Capital Territory and Tasmania includes similar offence provisions to those in Queensland.[403]

[3.164] In contrast, the surveillance devices legislation in the Northern Territory, Victoria and Western Australia contains a single offence provision, with several exceptions. Generally, a person is prohibited from communicating or publishing a record or report of a private conversation or private activity, which is known about, or which the person knows has been made, as a direct or indirect result of the use of a listening device, an optical surveillance device or, except for Western Australia, a

401 Or to communicate or publish a statement prepared from such a record: *Invasion of Privacy Act 1971* (Qld) s 45(1).

402 *Invasion of Privacy Act 1971* (Qld) s 45(2).

403 *Listening Devices Act 1992* (ACT) ss 5(1), 6(1); *Listening Devices Act 1991* (Tas) ss 9(1), 10(1).

tracking device.[404] These offences apply in relation to both lawful and unlawful use of those devices.[405]

[3.165] The surveillance devices legislation in New South Wales contains a similar offence provision, except that it is limited to the communication or publication of information about a private conversation or the carrying on of an activity, which is known about (directly or indirectly) through the unlawful use of a listening device, an optical surveillance device or a tracking device.[406] It also contains a separate offence provision, which prohibits a person from communicating or publishing information regarding the input of information into, or the output of information from, a computer, obtained from the unlawful use of a data surveillance device.[407]

[3.166] In South Australia, it is an offence for a person to communicate or publish information or material derived from the unlawful use of a surveillance device.[408] It is also an offence for a person to communicate or publish information or material derived from the use of a listening device or an optical surveillance device in circumstances where the device was lawfully used to protect the lawful interests of that person, or in the public interest.[409]

[3.167] The communication or publication prohibitions and their exceptions in each of the Australian jurisdictions is summarised in the following table and considered in more detail in the discussion that follows.

---

404 *Surveillance Devices Act* (NT) s 15(1); *Surveillance Devices Act 1999* (Vic) s 11(1); *Surveillance Devices Act 1998* (WA) s 9(1). A 'record' includes an audio, visual or audio visual record, a record in digital form, or a documentary record or statement prepared from such a record. A 'report' includes a report of the substance, meaning or purport of the conversation or activity. For the meaning of 'private conversation' and 'private activity' see [2.75]–[2.76] above.

405 In Victoria and Western Australia, it is an offence if the communication or publication is done 'knowingly'. In Western Australia, the record or report must have come to the person's knowledge as a direct or indirect result of the use of a surveillance device. In the Northern Territory, the person must know the record or report has been made as a direct or indirect result of the use of a relevant device.

406 *Surveillance Devices Act 2007* (NSW) ss 11(1). However, the legislation regulates the use of an optical surveillance device only to the extent that it involves entry into a building or vehicle, or interference with a vehicle or other object, without consent. See [2.74], [3.76] above.

407 *Surveillance Devices Act 2007* (NSW) s 14(1). Similar provision is made in the legislation in the Northern Territory and Victoria, but is limited to the use of data surveillance devices by law enforcement officers and extends to lawful and unlawful use: *Surveillance Devices Act* (NT) s 16; *Surveillance Devices Act 1999* (Vic) s 12. In Queensland, the *Police Powers and Responsibilities Act 2000* (Qld) prohibits the communication or publication of 'protected information', which includes any information obtained from the use of a surveillance device under a warrant or relevant authorisation: ss 351 (definition of 'protected information'), 352.

408 *Surveillance Devices Act 2016* (SA) s 12(1).

409 *Surveillance Devices Act 2016* (SA) ss 9(1), 10(1).

	QLD	ACT	NSW	NT	SA	TAS	VIC	WA
General restriction on communication or publication of information obtained through use of surveillance device by—[410]								
any person	✓	✓	✓	✓	✓	✓	✓	✓ (not tracking devices)
a party to the private conversation	✓	✓				✓		
Exceptions/circumstances where communication or publication may be made—[411]								
with consent of other parties to the private conversation or activity	✓ (by a person with consent of a party; by a party with consent of all other parties)	✓ (all principal parties)	✓ (all principal parties; or for data surveillance device— person having lawful possession or control of the computer)	✓ (all parties)	✓ (all parties)	✓ (all principal parties)	✓ (all parties)	✓ (all principal parties)
to a party to the private conversation or activity	✓	✓	✓ (or for data surveillance device— to the person having lawful possession or control of the computer)		✓	✓		✓
in some or all legal proceedings	✓	✓	✓	✓	✓	✓	✓	✓
to protect that person's lawful interests	✓ (only by a party)	✓ (by a party; or by a person where device used with consent of principal party to protect the lawful interests of that party)		✓	✓[412] (permitted in particular circumstances where listening or optical surveillance device used to protect lawful interests)	✓ (only by a party)	✓	✓ (or where device used with consent of principal party to protect the lawful interests of that party)
for safety or wellbeing, eg. imminent threat of serious violence			✓			✓		✓

410 In some jurisdictions, the prohibition applies only where the information was obtained by the unlawful use of a surveillance device. In some other jurisdictions, it applies whether the use was lawful, unlawful or unintentional. In addition, some exceptions apply differently depending on whether the person was a party to the relevant conversation or activity.

411 In Western Australia, it is a requirement that the communication or publication is not more than is reasonably necessary in the public interest, in the performance of a duty of the person making it, or for the protection of the lawful interests of the person making it. It is also a requirement that it is made to a person who has, or is believed on reasonable grounds to have, such an interest in the private conversation or activity as to make the publication or communication reasonable under the circumstances under which it is made: *Surveillance Devices Act 1998* (WA) s 9(3)(a)–(b).

412 To see the circumstances in which this is permitted, see [3.180] below. Generally, where a person has used a listening device or optical surveillance device to protect their lawful interests, communication or publication is permitted in several of the specific circumstances listed in the table. There are also limited exceptions in South Australia for private investigators.

	QLD	ACT	NSW	NT	SA	TAS	VIC	WA
in the public interest	✓ (only by a party)			✓ (by a person; or with a court order)	✓ (where listening or optical surveillance device used— to a media organisation; by a media organisation; or with a court order)		✓	✓ (only with a court order)
in the performance of a duty	✓ (only by a party)				✓			✓
to a person with a reasonable interest	✓ (only by a party)	✓ (only by a party)				✓ (only by a party)		
where knowledge obtained other than by unlawful use	✓	✓	✓		✓	✓		

[3.168] Some exceptions relate to specific persons who are authorised by law to use a relevant surveillance device, including law enforcement officers.[413] Other exceptions, such as the public interest exception, apply more generally.

Exceptions: where a communication or publication is permitted

Communication or publication to a party, or with consent of parties

[3.169] In Queensland, it is not an offence for a person to communicate or publish information about a private conversation obtained through the unlawful use of a listening device if the communication or publication is made to a party to the conversation or with the consent, express or implied, of such a party.[414] It is also not an offence for a party to a private conversation to communicate or publish information obtained through the use of a listening device if it is made to another party to the private conversation, or with the consent of all other persons by or to whom words are spoken in the course of the private conversation.[415]

413 See, eg, *Invasion of Privacy Act 1971* (Qld) s 45(2)(e); *Listening Devices Act 1992* (ACT) ss 5(2)(f), (3); *Surveillance Devices Act* (NT) ss 15(2)(d)–(f), 16; *Surveillance Devices Act 2016* (SA) ss 9(1)(h), 12(2)(e); *Listening Devices Act 1991* (Tas) ss 9(3), 10(2)(e), (3); *Surveillance Devices Act 1999* (Vic) ss 11(2)(ca)–(d), (f), 12; *Surveillance Devices Act 1998* (WA) s 9(2)(a)(iii)–(iv). Provisions in the Northern Territory and Victoria relating to the communication or publication of information obtained from the use of a data surveillance device are limited to law enforcement officers and are not included in the table or the discussion. The terms of reference exclude the use of surveillance devices for State law enforcement purposes from this review: see terms of reference, para E.

414 *Invasion of Privacy Act 1971* (Qld) s 44(2)(a)(i). A 'party' includes a person by or to whom words are spoken in the course of a private conversation (referred to in some other jurisdictions as a 'principal party'), and a person who overhears, records, monitors of listen to those words with the consent of any of those persons: s 42(2). See [2.66] above.

415 *Invasion of Privacy Act 1971* (Qld) s 45(2)(a). For the purposes of this provision, consent is required from each person by or to whom words are spoken in the course of the private conversation: s 42(2)(a).

[3.170] The surveillance devices legislation in each of the other states and territories similarly provides that a person does not commit an offence if the communication or publication is made with the consent of all the parties (or, in the Australian Capital Territory, New South Wales, Tasmania and Western Australia, all the principal parties) to the private conversation or activity.[416] Except in the Northern Territory and Victoria, the legislation also provides that it is not an offence if the communication or publication is made to a party to the private conversation or activity.[417]

[3.171] In New South Wales, it is not an offence to communicate or publish information obtained from the use of a data surveillance device if it is made to the person having lawful possession or control of the computer, or with the consent of that person.[418]

Communication or publication in the course of legal proceedings

[3.172] The communication or publication prohibitions in surveillance devices legislation apply to communication or publication to a court.[419] However, in each jurisdiction, such communication or publication is permitted in the course of some, or all, legal proceedings.[420]

[3.173] In Queensland, a person who is not a party to a private conversation may communicate or publish information about a private conversation obtained through the unlawful use of a listening device only in the course of proceedings for an offence against part 4 of the *Invasion of Privacy Act 1971*.[421]

[3.174] A person who is a party to a private conversation may communicate or publish information obtained through the use of a listening device in the course of legal proceedings.[422] 'Legal proceedings' is defined to include civil or criminal proceedings in or before any court, proceedings before justices, proceedings before any court, tribunal or person (including any inquiry, examination or arbitration) in which evidence is or may be given, and any part of legal proceedings.[423]

---

416 For a discussion of the meaning of 'party' and 'principal party', see [2.77]–[2.78] above.

417 *Listening Devices Act 1992* (ACT) ss 5(2)(a),(b), 6(2)(a)(i),(ii); *Surveillance Devices Act 2007* (NSW) s 11(2)(a)(i),(ii); *Surveillance Devices Act* (NT) s 15(2)(a); *Surveillance Devices Act 2016* (SA) ss 9(1)(a), (b), 12(2)(a), (b); *Listening Devices Act 1991* (Tas) ss 9(2)(a)(i),(ii), 10(2)(a); *Surveillance Devices Act 1999* (Vic) s 11(2)(a); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(i),(ii).

418 *Surveillance Devices Act 2007* (NSW) s 14(2)(a)(i),(ii).

419 See *Thomas v Nash* (2010) 107 SASR 309, [54]–[55] (Doyle CJ) in which it was held that evidence of a private conversation recorded without the consent of the other participants was inadmissible, because the communication or publication prohibition in s 5 of the *Listening and Surveillance Devices Act 1972* (SA) applied to communication or publication to a court.

420 Surveillance devices legislation in some jurisdictions also includes separate provisions in relation to the inadmissibility of evidence. See [3.207]–[3.208] below.

421 *Invasion of Privacy Act 1971* (Qld) s 44(2)(a)(ii).

422 *Invasion of Privacy Act 1971* (Qld) s 45(2)(b).

423 *Invasion of Privacy Act 1971* (Qld) s 45(3).

[3.175] Similar exceptions are included in surveillance devices legislation in the Australian Capital Territory and Tasmania.[424]

[3.176] The surveillance devices legislation in the remaining jurisdictions variously permits communication or publication by a person:[425]

- in the course of proceedings for an offence against the surveillance devices legislation (New South Wales, South Australia);[426] or
- in the course of legal proceedings (Northern Territory, Victoria, Western Australia).[427]

Communication or publication to protect a person's lawful interests

[3.177] In Queensland, it is not an offence for a party who has used a listening device to communicate or publish a record of a private conversation if that communication or publication is 'not more than is reasonably necessary for the protection of the lawful interests of that person'.[428]

[3.178] Similar provision is made in most other jurisdictions, if the communication or publication is reasonably necessary (or not more than is reasonably necessary) to protect the lawful interests of the person making it.[429]

[3.179] As explained above, the term 'lawful interests' is not defined in the legislation. A person's lawful interests are to be determined on the facts of each case.[430] However, the requirement for the communication or publication to be 'reasonably necessary' to protect the person's lawful interests necessitates an evaluation of the purposes for which the communication or publication is carried out and whether it is necessary and proportionate, given the intent of the legislation to protect personal privacy.[431]

---

424 *Listening Devices Act 1992* (ACT) ss 5(2)(c), 6(2)(a)(iii); *Listening Devices Act 1991* (Tas) s 9(2)(a)(iii), s 10(2)(b). In the Australian Capital Territory, the exception for communication or publication by a party applies to any 'civil or criminal proceedings'.

425 *Surveillance Devices Act 2007* (NSW) ss 11(2)(a)(iv), 14(2)(a)(iv); *Surveillance Devices Act* (NT) s 15(2)(c); *Surveillance Devices Act 2016* (SA) s 12(2)(d); *Surveillance Devices Act 1999* (Vic) s 11(2)(c); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(ix).

426 An exception also expressly permits communication or publication for the purpose of investigating or prosecuting such an offence: *Surveillance Devices Act 2007* (NSW) ss 11(2)(a)(iii), 14(2)(a)(iii); *Surveillance Devices Act 2016* (SA) ss 9(1)(c)–(d), 12(2)(c).

427 The precise wording is: 'in the course of legal or disciplinary proceedings' (Northern Territory, Victoria); 'in the course of any legal proceedings' (Western Australia).

428 *Invasion of Privacy Act 1971* (Qld) s 45(2)(c)(iii).

429 *Listening Devices Act 1992* (ACT) s 5(2)(d); *Surveillance Devices Act* (NT) s 15(2)(b)(ii); *Listening Devices Act 1991* (Tas) s 10(2)(c); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(ii); *Surveillance Devices Act 1998* (WA) s 9(2)(vi), (3)(a)(iii). In the Australian Capital Territory and Western Australia, where a listening device is used with the consent of a principal party to protect their lawful interests, a communication or publication may be made in the course of reasonable action taken to protect the lawful interests of the consenting principal party: *Listening Devices Act 1992* (ACT) s 6(2)(a)(iv); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(vii).

430 See [3.110]–[3.112] above.

431 ACT Review (2016) [6.15].

[3.180] In South Australia, surveillance devices legislation does not contain a broad exception where communication or publication is made to protect a person's lawful interests.[432] Instead, the legislation provides that a person must not knowingly use, communicate or publish information or material derived from the use of a listening device or an optical surveillance device in circumstances where the device was used to protect the lawful interests of that person, except:[433]

> (a) to a person who was a party to the conversation or activity to which the information or material relates; or
>
> (b) with the consent of each party to the conversation or activity to which the information or material relates; or
>
> (c) to an officer of an investigating agency for the purposes of a relevant investigation or relevant action or proceeding; or
>
> (d) in the course, or for the purposes, of a relevant action or proceedings;[434] or
>
> (e) in relation to a situation where—
>
> (i) a person is being subjected to violence; or
>
> (ii) there is an imminent threat of violence to a person; or
>
> (f) to a media organisation; or
>
> (g) in accordance with an order of a judge under [part 2 division 2 of this Act];[435] or
>
> (h) otherwise in the course of duty or as required or authorised by law. (notes added)

Communication or publication by a private investigator or loss adjuster

[3.181] In South Australia, a licensed investigation agent or loss adjuster must not knowingly communicate or publish information derived from the lawful use of a listening device or optical surveillance device, except to a prescribed person or class of persons, in prescribed circumstances, or as authorised under the Act or any other Act or law.[436]

[3.182] For a licensed investigation agent:[437]

---

432 Such an exception was considered 'too broad': see [3.96] above.

433 *Surveillance Devices Act 2016* (SA) s 9(1).

434 A 'relevant action or proceeding' is defined to include a prosecution of an offence, an application for bail, and other specified proceedings or hearings: s 3(1).

435 A person may apply to a Judge of the Supreme Court of South Australia for an order authorising the communication or publication of information or material derived from the use of a listening device or an optical surveillance device: *Surveillance Devices Act 2016* (SA) s 11(1).

436 *Surveillance Devices Act 2016* (SA) s 9(2), (3). Broadly, the circumstances in which a private investigator or loss adjuster may lawfully use a surveillance device relate to the public interest and the protection of lawful interests. As to licensed investigation agents and loss adjusters, see [3.145] above.

437 *Surveillance Devices Regulations 2017* (SA) s 12.

- prescribed persons or classes of persons include the clients or employers of the licensed investigation agent and the legal representatives and medical practitioners of those clients or employers; and
- prescribed circumstances include:
  - the communication of information or material to another licensed investigation agent employed by the same employer or client for the purpose of briefing the other agent about matters relating to that employer or client;
  - the communication of information or material to an officer of an investigating agency for the purposes of a relevant investigation or relevant action or proceeding; or
  - the reasonable communication of information or material to a person in order to assist the licensed investigation agent with an investigation.

Communication or publication for safety and well-being

[3.183] The surveillance devices legislation in New South Wales, Tasmania, and Western Australia permits the communication or publication of information obtained from the use of a surveillance device:[438]

- if it is made in connection with an imminent threat of serious violence or substantial damage to property, or the commission of a serious narcotics offence (New South Wales and Tasmania) and is no more than is reasonably necessary (New South Wales) or if the person believes on reasonable grounds that it is necessary (Tasmania); or
- if it is made to police in connection with an indictable drug offence or other serious indictable offence, or if a person believes on reasonable grounds that it is necessary in connection with an imminent threat of serious violence or substantial damage to property (Western Australia).

[3.184] In South Australia, the communication or publication of information or material obtained from the use of a listening device or optical surveillance device to protect a person's lawful interests is permitted in relation to a situation where a person is being subjected to violence or there is an imminent threat of violence to a person.[439]

Communication or publication in the public interest

[3.185] The legislation in Queensland, the Northern Territory and Victoria contains a broad public interest exception.[440]

---

438 *Surveillance Devices Act 2007* (NSW) ss 11(2)(b), 14(2)(b); *Listening Devices Act 1991* (Tas) s 9(2)(b); *Surveillance Devices Act 1998* (WA) s 9(2)(b), (c). See also *Surveillance Devices Act 1999* (Vic) s 11(2)(e) in relation to a communication to a police officer.

439 *Surveillance Devices Act 2016* (SA) s 9(1)(e).

440 As to the use of a surveillance device in the 'public interest', see [3.120] ff above.

[3.186] In Queensland, a party who has used a listening device will not commit an offence by communicating or publishing a record of a private conversation if that communication or publication is 'not more than is reasonably necessary in the public interest'.[441]

[3.187] Similar provision—for communication or publication by a person that is 'reasonably necessary in the public interest'—operates in the Northern Territory and Victoria.[442]

[3.188] The public interest exception may, for example, apply in relation to a media organisation, journalist, private investigator or loss adjuster.[443]

[3.189] In the Northern Territory, South Australia and Western Australia, an order of a Supreme Court Judge is required prior to communication or publication in the public interest.[444]

[3.190] The requirement for judicial oversight in these circumstances:[445]

> ensures that the privacy of the public is maintained not only at the time of surveillance, but also after any surveillance recording has been made.

[3.191] In South Australia, the requirement for an order of a Supreme Court Judge does not apply if the communication or publication is made:[446]

- to a media organisation; or
- by a media organisation and the information or material is in the public interest.

[3.192] The exceptions for a media organisation were included following opposition to an earlier Bill that required, as a blanket rule, an order of a Supreme Court Judge

---

441 *Invasion of Privacy Act 1971* (Qld) s 45(2)(c)(i).

442 *Surveillance Devices Act* (NT) s 15(2)(b)(i); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(i). In Victoria, the communication or publication must be no more than is reasonably necessary.

443 As to private investigators in Queensland, see [3.142]–[3.143] above.

444 *Surveillance Devices Act* (NT) s 46; *Surveillance Devices Act 1998* (WA) ss 9(2)(a)(viii), 31(1) and *Interpretation Act 1984* (WA) s 5 (definition of 'judge'); *Surveillance Devices Act 2016* (SA) ss 3(1) (definition of 'judge'), 10(1). In the Northern Territory, this requirement does not apply in all circumstances.

In Western Australia, the legislation states that an exception to the prohibition on communication or publication applies only if the relevant communication or publication 'is not more than is reasonably necessary in the public interest': *Surveillance Devices Act 1998* (WA) s 9(3)(a)(i).

445 Western Australia, *Parliamentary Debates*, Legislative Council, 21 October 1998, 2406 (NF Moore, Leader of the House).

446 *Surveillance Devices Act 2016* (SA) s 10(2). 'Media organisation' is defined in s 3(1) to mean 'an organisation whose activities consist of or include the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs, information or a documentary;

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs, information or a documentary'.

Communication or publication to a media organisation is also permitted where the surveillance was conducted to protect a person's lawful interests: s 9(1)(f).

prior to any communication or publication of information obtained from the use of a relevant surveillance device in the public interest.[447]

[3.193] The scope of the public interest exception in surveillance devices legislation has been considered in some law reform reviews and inquiries.

[3.194] The NSWLRC considered that an open-ended public interest exception in relation to covert surveillance 'would be too broad, would be open to abuse and would offer insufficient privacy safeguards':[448]

> Where definitions of public interest have been attempted, they have necessarily been vague and wide-ranging, and would potentially encompass any type of situation. The Commission is of the view that, because public interest is such a nebulous concept, surveillance legislation which contained a broad exception without requiring approval by an issuing authority would operate so broadly that it would not operate as a proper curb on unwarranted intrusions into personal privacy. The public interest in preventing illegality, protecting legitimate rights and interests or providing the public with information does not and should not automatically take precedence over privacy concerns in every situation. Covert surveillance may sometimes be justified in circumstances which involve the public interest. Covert surveillance will, however, always be a breach of privacy. Introducing a broad public interest exception with no approval process into surveillance legislation would have the effect of condoning covert surveillance in all cases where the person or organisation conducting the surveillance believes there to be a public interest involved, regardless of the privacy ramifications. (note omitted)

[3.195] Accordingly, it recommended that the communication or publication of information obtained through covert surveillance should always require authorisation. As explained above, it recommended a new scheme for the authorisation of covert surveillance conducted in the public interest, similar to the process for authorising covert surveillance by law enforcement officers.[449]

[3.196] The NSWLRC considered whether a special exception should apply in relation to covert surveillance by a media organisation, but ultimately concluded that it should not, stating:[450]

> The Commission acknowledges that failing to exempt the media from its proposed regulatory scheme will generate controversy. However, the Commission does not accept the argument that including the media within the

---

447 South Australia, *Parliamentary Debates*, House of Assembly, 10 September 2015, 2477 (JR Rau, Deputy Premier, Attorney-General, Minister for Justice Reform, Minister for Planning, Minister for Housing and Urban Development, Minister for Industrial Relations, Minister for Child Protection Reform). See also [3.120] ff, [3.145] above as to use by a private investigator or loss adjuster in the public interest.

448 NSWLRC Report No 98 (2001) [6.24]–[6.25].

449 Ibid [2.60], Recs 49, 55, 81, 82. The NSWLRC recommended that the 'proposed legislation should contain a separate part applying to anyone (including the media) wishing to conduct surveillance in the public interest, but should require authorisation prior to conducting the surveillance, rather than before publication occurs'. The NSWLRC affirmed these recommendations in NSWLRC Report No 108 (May 2005) [5.37]–[5.49], but they have not been implemented. As to the authorisation process recommended by the NSWLRC, see [3.130]–[3.132] above, [D.7] below.

450 NSWLRC Report No 98 (2001) [2.61]. See also [6.16]–[6.18]. The NSWLRC noted that the authorisation process would only apply to covert surveillance, 'due to its highly intrusive nature'. It also noted that the use of covert surveillance by the media 'is carried out rarely, and only as a last resort', so that the requirement for an authorisation would affect 'only a small part of the media's operations': [6.19].

> scope of new surveillance laws will act as a curb on freedom of speech or expression. It will merely ensure that, in upholding freedom of speech, the media respect other equally important public interests and act in accordance with the law.

[3.197] The ALRC recommended that, instead of a broad public interest defence, surveillance devices legislation should provide a 'responsible journalism' defence 'relating to matters of public concern and importance'.[451] Such a defence would apply to offences in relation to the installation or use of a surveillance device as well as to the communication of information obtained through surveillance. However, a distinction was drawn in relation to how this defence would apply to these offences:[452]

> The circumstances that justify communication of information obtained through surveillance may be different from those that justify the installation or use of a surveillance device. A journalist is unlikely to know what information will be obtained under surveillance before the surveillance is completed—for example, a public official may or may not make a comment that suggests corruption during a particular recording.
>
> A responsible journalism defence to the installation or use of a surveillance device should therefore depend on whether it was reasonable for the journalist to believe that the use of the surveillance device was in the public interest, and not on whether the information obtained through surveillance was, in hindsight, information in the public interest. However, considerations of whether the information obtained was in the public interest may be relevant if a responsible journalism defence is to be applied to the use or communication of information obtained through surveillance, rather than the act of surveillance itself.

[3.198] In the ACT Review, it was recommended that the legislation should:[453]

> allow surveillance when it is carried out to protect a public interest and the surveillance activity is necessary and proportionate. Communication of the results of surveillance should require a court order unless the communication is to a media organisation subject to an appropriate code of conduct.

[3.199] The AAUS and Liberty Victoria considered that there should be an exception 'in the public interest' for the communication or publication of information obtained through the unlawful use of a surveillance device without consent.[454]

Communication or publication in the performance of a duty

[3.200] In Queensland, a party who has used a listening device will not commit an offence by communicating or publishing a record of the private conversation if that communication or publication is 'not more than is reasonably necessary in the performance of a duty of [that] person'.[455]

---

451 ALRC Report No 123 (June 2014) [14.58]–[14.76], Rec 14-5. See [3.133]–[3.134] above.

452 Ibid [14.61]–[14.62].

453 ACT Review (2016) [2.5](d), [6.21].

454 AAUS and Liberty Victoria Paper (2015) Rec 5.

455 *Invasion of Privacy Act 1971* (Qld) s 45(2)(c)(ii).

[3.201] Similarly, in South Australia and Western Australia, the offence does not apply where a person makes a publication or communication in the course of their duty.[456] In Western Australia, the publication or communication must be not more than is reasonably necessary in the performance of the duty.[457]

Communication or publication to a person with a reasonable interest in the circumstances

[3.202] In Queensland, it is not an offence for a party who has used a listening device to communicate or publish a record of a private conversation to a person who has, or who the party believes on reasonable grounds to have, 'such an interest in the private conversation as to make the communication or publication reasonable under the circumstances in which it is made'.[458]

[3.203] Similar provision is made in the surveillance devices legislation in the Australian Capital Territory, and Tasmania.[459]

[3.204] In Western Australia, it is a general requirement of any defence of communication or publication that it is made to a person who has, or is believed on reasonable grounds by the person making the publication or communication to have, such an interest in the private conversation or activity as to make the communication or publication reasonable under the circumstances in which it is made.[460]

Communication or publication by a person who obtained knowledge other than by unlawful use of the device

[3.205] In Queensland, a person is not prohibited from communicating or publishing knowledge of a private conversation that was not obtained through the unlawful use of a surveillance device, even if that person also obtained knowledge of the conversation through the unlawful use of a surveillance device.[461]

[3.206] Similar provision is included in some other jurisdictions.[462] By way of example, the legislation in South Australia states that if knowledge of information or material is obtained in a manner that does not contravene the law about surveillance devices, then the person is not prohibited from communicating or publishing their knowledge of that information or material (even if the same knowledge was also obtained in a manner that contravened the law). The Law Society of South Australia explained that they understood this provision as:[463]

---

456 *Surveillance Devices Act 2016* (SA) ss 9(1)(h), 12(2)(e); *Surveillance Devices Act 1998* (WA) s 9(2)(v).

457 *Surveillance Devices Act 1998* (WA) s 9(3)(a)(ii).

458 *Invasion of Privacy Act 1971* (Qld) s 45(2)(d).

459 *Listening Devices Act 1992* (ACT) s 5(2)(e); *Listening Devices Act 1991* (Tas) s 10(2)(d).

460 *Surveillance Devices Act 1998* (WA) s 9(3)(b).

461 *Invasion of Privacy Act 1971* (Qld) s 44(2)(b).

462 *Listening Devices Act 1992* (ACT) s 6(2)(b); *Surveillance Devices Act 2007* (NSW) ss 11(3), 14(3); *Surveillance Devices Act 2016* (SA) s 12(3); *Listening Devices Act 1991* (Tas) s 9(2)(c).

463 SA Legislative Review Committee Report (2013) 28, referring to the submission made to the Committee by the Law Society of South Australia.

> Favoring the *public interest* in free expression over the private interest in privacy by inherently permitting information unlawfully obtained to be later communicated if that same information can also be obtained from a lawful source. (emphasis in original)

Admissibility of evidence obtained from surveillance device

[3.207] In Queensland, the *Invasion of Privacy Act 1971* expressly provides that a person who has knowledge of a private conversation as a direct or indirect result of the unlawful use of a listening device may not give evidence of that conversation in any civil or criminal proceedings.[464] That evidence is only admissible where:[465]

- a party to the conversation consents to the person giving evidence;
- the person giving evidence has obtained knowledge of the conversation in the way described and also in some other way; or
- the evidence is given in proceedings for an offence against the *Invasion of Privacy Act 1971* that is constituted by a contravention of, or failure to comply with, any provision in the part of the Act about listening devices.[466]

[3.208] Similar provision, although varying in terms and scope, is made in the Australian Capital Territory and Tasmania.[467] At the time this provision was enacted in the Australian Capital Territory, it was considered that 'the inadmissibility of evidence obtained by the unlawful use of a listening device will be the most effective means of deterring and eliminating' covert surveillance.[468]

[3.209] Surveillance devices legislation in other jurisdictions does not contain similar provisions about the inadmissibility of evidence, generally leaving the admissibility of evidence unlawfully obtained to the court's discretion.[469] In New South Wales, the Northern Territory and Victoria, the legislation expressly provides that it 'is not intended to limit a discretion that a court has to admit or exclude evidence in any proceeding'.[470]

---

464 *Invasion of Privacy Act 1971* (Qld) s 46(1).

465 *Invasion of Privacy Act 1971* (Qld) s 46(2).

466 The relevant part of the *Invasion of Privacy Act 1971* (Qld) is pt 4. In such proceedings, the court may make an order that forbids the publication of the evidence or any report about that evidence. Contravention of such an order is an offence for which the maximum penalty is 10 penalty units ($1305.50): *Invasion of Privacy Act 1971* (Qld) s 46(3)–(4).

467 *Listening Devices Act 1992* (ACT) s 10; *Listening Devices Act 1991* (Tas) s 14.

468 ACT, Legislative Assembly, *Parliamentary Debates*, 20 August 1992, 1880 (Connolly, Attorney-General, Minister for Housing and Community Services and Minister for Urban Services).

469 In some jurisdictions, there are specific provisions relevant to the inadmissibility of evidence obtained pursuant to a warrant or authorisation, or in other relevant similar circumstances: see, eg, *Surveillance Devices Act* (NT) s 70; *Listening Devices Act 1991* (Tas) ss 14(2), 15; *Surveillance Devices Act 1998* (WA) ss 10, 11.

470 *Surveillance Devices Act 2007* (NSW) s 3(2)(a); *Surveillance Devices Act* (NT) s 10(1)(a); *Surveillance Devices Act 1999* (Vic) s 5A(1)(a). In Queensland, s 10 of the *Police Powers and Responsibilities Act 2000* (Qld) similarly provides that the Act 'does not affect the common law under which a court in a criminal proceeding may exclude evidence in the exercise of its discretion'.

[3.210] At common law, a court has discretion to exclude evidence that has been obtained unlawfully or unfairly:[471]

> Evidence of relevant facts or things ascertained or procured by means of unlawful or unfair acts is not, for that reason alone, inadmissible … On the other hand evidence of facts or things so ascertained or procured is not necessarily to be admitted, ignoring the unlawful or unfair quality of the acts by which the facts sought to be evidenced were ascertained or procured. Whenever such unlawfulness or unfairness appears, the judge has a discretion to reject the evidence. He must consider its exercise. In the exercise of it, the competing public requirements must be considered and weighed against each other. On the one hand there is the public need to bring to conviction those who commit criminal offences. On the other hand there is the public interest in the protection of the individual from unlawful and unfair treatment …

[3.211] Generally, where evidence is obtained by an unlawful act in contravention of legislation, this factor may 'more readily warrant' the court exercising their discretion to reject the evidence. Alternatively, legislation may impliedly forbid the use of facts or things that were obtained in a way that breaches that legislation.[472]

[3.212] The Australian Capital Territory, New South Wales, the Northern Territory, Tasmania and Victoria have enacted uniform evidence legislation that contains a statutory discretion to exclude improperly or illegally obtained evidence in court proceedings.[473]

[3.213] The surveillance devices legislation in New South Wales previously included a provision limiting the admissibility of evidence of a private conversation unlawfully obtained, similar to the existing provisions in Queensland, the Australian Capital Territory and Tasmania.[474] However, this provision was repealed by the current legislation. The NSWLRC observed that 'provision exists under the *Evidence Act 1995* (NSW) for the court to exclude improperly or illegally obtained evidence'.[475]

[3.214] In the recent ACT Review it was observed that the express provision in the surveillance devices legislation in that jurisdiction restricting the use of evidence obtained using a listening device 'displaces the more general provision for adducing

---

471 The Hon JD Heydon AC, LexisNexis, *Cross on Evidence*, (at September 2018) [27240], [27245], referring to *Bunning v Cross* (1978) 141 CLR 54, 72. However, if legislation expressly prohibits the communication of unlawfully obtained evidence to the court, 'no question of discretion arises: the evidence cannot be received': [27270], citing *Thomas v Nash* (2010) 107 SASR 309. The court's discretion as to the admissibility of evidence therefore also relates to the scope of the communication and publication prohibition (and, in particular, the extent of any exception for communication and publication in the course of legal proceedings). This is discussed at n 419 above.

472 Ibid [27245], referring to *Hilton v Wells* (1985) 157 CLR 57, 77.

473 *Evidence Act 2011* (ACT) s 138; *Evidence Act 1995* (NSW) s 138; *Evidence (National Uniform Legislation) Act* (NT) s 138; *Evidence Act 2001* (Tas) s 138; *Evidence Act 2008* (Vic) s 138.

474 *Listening Devices Act 1984* (NSW) (repealed) s 13.

475 NSWLRC, Issues Paper No 12 (1997) [5.24].

improperly or illegally obtained evidence'.[476] It was recommended that the admission of evidence should be left to the court's discretion.[477]

Questions

Q-15 Should there be a general prohibition on the communication or publication of information obtained through the unlawful use of a surveillance device? Why or why not?

Q-16 If 'no' to Q-15, should the communication or publication of information obtained through the unlawful use of a surveillance device be prohibited in particular circumstances, for example, if the communication of publication is not made:

- **(a) to a party or with the consent of the parties to the private conversation or activity;**
- **(b) in the course of legal proceedings;**
- **(c) to protect the lawful interests of the person making it;**
- **(d) in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;**
- **(e) in the public interest;**
- **(f) in the performance of a duty;**
- **(g) to a person with a reasonable interest in the circumstances;**
- **(h) by a person who obtained knowledge other than by use of the device; or**
- **(i) in any other circumstances?**

Q-17 Should there be a general provision permitting the communication or publication of information obtained through the lawful use of a surveillance device? Why or why not?

Q-18 If 'no' to Q-17, should the communication or publication of information obtained through the lawful use of a surveillance device be permitted in particular circumstances, for example, if the communication or publication is made:

476 ACT Review (2016) [6.41].

477 Ibid [6.45]. In particular, it recommended that 'a court should have a discretion to admit evidence obtained through use [of] a surveillance device where the recording was intended at the time of the recording, whether reasonably or not, to be used to protect a principal party's lawful interests'.

(a) to a party or with the consent of the parties to the private conversation or activity;

(b) in the course of legal proceedings;

(c) to protect the lawful interests of the person making it;

(d) in the public interest;

(e) in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;

(f) in the performance of a duty;

(g) to a person with a reasonable interest in the circumstances;

(h) by a person who obtained knowledge other than by use of the device; or

(i) in any other circumstances?

Q-19 Should any special provision be made in relation to the communication or publication of information obtained through the prohibited or permitted use of a surveillance device:

(a) by a journalist or media organisation;

(b) by a private investigator;

(c) by a loss adjuster; or

(d) in any other circumstances?

If so, what provision should be made and why?

Admissibility of evidence obtained from surveillance device

Q-20 How should the admissibility of evidence, in court proceedings, of information obtained by the unlawful use of a surveillance device be dealt with?

Penalties and remedies

Criminal penalties

[3.215] The *Invasion of Privacy Act 1971* contains a number of prohibitions, as discussed above. These are framed as criminal offences.

[3.216] The use prohibition and the communication or publication prohibitions are indictable offences. The maximum prescribed penalty for those offences is 40 penalty units ($5222) or 2 years imprisonment.[478]

[3.217] Charges and convictions for those offences are relatively infrequent.[479]

[3.218] Other offences against the Act are punishable on summary conviction[480] and attract a lesser maximum penalty ranging from 10 penalty units ($1305.50) to 30 penalty units ($3916.50) or 18 months imprisonment.[481] These offences are subject to a limitation period of 12 months from the commission of the alleged offence or 6 months after the commission of the alleged offence comes to the complainant's knowledge, whichever is the later.[482]

[3.219] The position is similar in other jurisdictions—the surveillance devices legislation in each of the other Australian states and territories and in New Zealand imposes criminal sanctions for breaches of the legislation.

---

478 *Invasion of Privacy Act 1971* (Qld) ss 43(1), 44(1), 45(1). These are misdemeanour offences: see s 49(2). The current prescribed value of a penalty unit is $130.55: *Penalties and Sentences Act 1992* (Qld) ss 5(1)(e)(i), 5A(1); *Penalties and Sentences Regulation 2015* (Qld) s 3.

479 Information provided by the Courts Performance and Reporting Unit, Queensland Courts Service, Department of Justice and Attorney-General, 11 December 2018. Between 2001–02 and 2018–19 (up to 31 October 2018), fewer than 18 defendants were lodged in Queensland courts charged with an offence against the *Invasion of Privacy Act 1971* (Qld) s 43(1), and no defendants were recorded for offences against ss 44(1) or 45(1):

	Use prohibition: s 43(1)		Communication or publication prohibitions: ss 44(1) and 45(1)	
	Charges	Convictions*	Charges	Convictions
Magistrates Court	13	<5	Nil	Nil
District Court	<5	<5	Nil	Nil

* At least two of those convictions resulted in a sentence of imprisonment.

480 See *Invasion of Privacy Act 1971* (Qld) s 49(3).

481 *Invasion of Privacy Act 1971* (Qld) ss 43(5) (breach of forfeiture order—20 penalty units), 46(4) (breach of non-publication order—10 penalty units), 48 (advertising listening device—20 penalty units or one year imprisonment), 48A(1), (1A), (3) (unlawful entry of dwelling house—20 penalty units or one year imprisonment or, in certain circumstances, 30 penalty units or 18 months imprisonment). See also s 49(1) which provides that the maximum penalty for a contravention of the Act which is not otherwise specifically provided for is 10 penalty units.

482 See *Invasion of Privacy Act 1971* (Qld) s 50.

[3.220] The maximum prescribed penalties for the primary offences under the legislation (for individuals) are as follows:[483]

	Use prohibitions	Communication or publication prohibitions
Qld	40 penalty units ($5222) or 2 years	40 penalty units ($5222) or 2 years
ACT	50 penalty units ($8000)	50 penalty units ($8000) or 6 months or both
NSW	100 penalty units ($11 000) or 5 years or both	100 penalty units ($11 000) or 5 years or both
NT	250 penalty units ($38 750) or 2 years	250 penalty units ($38 750) or 2 years
SA	$15 000 or 3 years	$15 000 or 3 years (where device used in breach of the Act) or $10 000 (in other specified cases)
Tas	40 penalty units ($6520) or 2 years or both	40 penalty units ($6520) or 2 years or both
Vic	240 penalty units ($38 686) or 2 years or both	240 penalty units ($38 686) or 2 years or both
WA	$5000 or 12 months or both	$5000 or 12 months or both
NZ	2 years	2 years

[3.221] In two jurisdictions—Tasmania and Western Australia—the surveillance devices legislation imposes a limitation period on the commencement of proceedings for an offence. In each case, the period is two years.[484]

[3.222] Criminal penalties include fines and imprisonment. A criminal court may also be empowered to make other orders, such as community based orders or orders for the forfeiture of property.[485] Convictions for criminal offences can also have significant indirect consequences, such as the requirement to disclose convictions when seeking certain types of employment, the disqualification of convicted persons from particular occupations, roles or entitlements, and the social stigma attached to having a criminal conviction.[486]

---

483 See *Listening Devices Act 1992* (ACT) ss 4(1), 5(1), 6(1) and *Legislation Act 2001* (ACT) s 133 (value of penalty unit $160 for individual and $810 for corporation); *Surveillance Devices Act 2007* (NSW) ss 7(1), 8(1), 9(1), 10(1), 11(1) and *Crimes (Sentencing Procedure) Act 1999* (NSW) s 17 (value of penalty unit $110); *Surveillance Devices Act* (NT) ss 11(1), 12(1), 13(1), 15(1) and *Penalty Units Regulation* (NT) reg 2 (value of penalty unit $155); *Surveillance Devices Act 2016* (SA) ss 4(1), 5(1)–(3), 7(1), 8(1), 9(1)-(3), 10(1), 12(1); *Listening Devices Act 1991* (Tas) s 12 and Tasmania, *Government Gazette* No 21 802, 30 May 2018, 569 (value of penalty unit $163); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1), 11(1) and Victoria, *Special Gazette* No 145, 29 March 2018 (value of penalty unit $161.19); *Surveillance Devices Act 1998* (WA) ss 5(1), 6(1), 7(1), 9(1); *Crimes Act 1961* (NZ) ss 216B(1), 216C(1).

484 *Listening Devices Act 1991* (Tas) ss 23, 24; *Surveillance Devices Act 1998* (WA) s 38. In Tasmania, the legislation also specifies that the consent of the Director of Public Prosecutions is required for proceedings to be instituted.

485 See generally the *Penalties and Sentences Act 1992* (Qld). Forfeiture orders are provided for under the *Invasion of Privacy Act 1971* (Qld) s 43(4): see [3.240] ff below.

486 See generally QLRC, *Expunging criminal convictions for historical gay sex offences*, Report No 74 (2016) [2.29]–[2.31], [2.36].

Civil penalties

[3.223] An alternative regulatory option for deterring and punishing breaches of the law is to provide for civil penalties, as opposed to (or in addition to) criminal sanctions.

[3.224] The *Invasion of Privacy Act 1971* does not impose any civil penalties. Neither does the surveillance devices legislation in other jurisdictions.

[3.225] Civil penalties—which are so named because they are imposed by civil rather than criminal court processes—are usually in the form of monetary penalties (fines). A court or tribunal might also be empowered to make other civil orders, such as injunctions.[487]

[3.226] Civil penalties can cover the same type of conduct as criminal offences. They may be considered appropriate for breaches that do not involve a fault element, such as intention or knowledge. They are often imposed for breaches by corporate entities, where imprisonment is not an option. Civil monetary penalties may in some cases be more substantial than criminal fines.[488]

[3.227] The main distinction between civil penalties and criminal penalties is the difference in the procedures by which they are enforced, as highlighted below:

	Criminal	Civil
Standard of proof	Criminal standard of 'beyond reasonable doubt'	Civil standard of the 'balance of probabilities'
Mental element	Usually a mental element to the offence such as intention or knowledge	Often no mental element to the conduct
Procedural protections	Right to remain silent (with limited exceptions where pre-trial disclosure obligations are imposed in some cases)	Extensive disclosure obligations
Decision-maker	Cases decided by a judicial officer and, in some cases, a jury	Cases decided by a judge or tribunal member, but rarely a jury
Orders	Fines, imprisonment and other sentencing options might be available	Usually a monetary penalty. Imprisonment not available.
Consequences	Criminal conviction which may need to be disclosed in various situations. May be disqualified from holding certain positions or deprived of certain entitlements.	Not a criminal conviction

[3.228] Provision for civil penalties is made in a number of Commonwealth and State Acts, including the *Privacy Act 1988* (Cth), *Competition and Consumer Act 2010* (Cth), *Banking Act 1959* (Cth), *Electricity Act 1994* and *Industrial Relations Act 2016*.

[3.229] The VLRC recommended the inclusion of civil penalties as an alternative to criminal penalties in the surveillance devices legislation, with the proposed regulator

487 See the discussion at [3.259] ff below.

488 See generally ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002) [2.16]–[2.19], [2.45]–[2.63], [2.107]–[2.115].

having the power to commence civil penalty proceedings. In making its recommendations, the VLRC observed that:[489]

> The commission has only been able to find evidence of four successful prosecutions for breach of the [*Surveillance Devices Act 1999* (Vic)] since its inception on 1 January 2000. All cases concerned the unlawful use of optical surveillance devices in particularly offensive circumstances. One explanation for the small number [of] prosecutions may be that the criminal sanctions in the [Act] are too severe for use in cases where the wrongful behaviour is not highly offensive.
>
> …
>
> the introduction of a civil penalty regime for existing offences in the [Act]… 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.
>
> Introducing civil penalties is also likely to reduce the cost and complexity of the regulatory process. (notes omitted)

[3.230] The AAUS and Liberty Victoria also proposed the use of civil penalties in surveillance devices legislation. In their view, civil penalties should attach to the use prohibition and the communication or publication prohibitions, with criminal penalties reserved as an alternative for the more serious proposed offence involving intimidation, harassment or harm.[490] In their view, civil penalties would:[491]

- likely reduce the cost and complexity of the regulatory process;
- invite the [proposed regulator] to act on less serious matters; and
- provide greater flexibility to best address the circumstances of each case.

Corporate and officer liability

[3.231] In most of the other jurisdictions, the surveillance devices legislation prescribes a higher maximum penalty if the offence is committed by a corporation:[492]

	Different penalty for a corporation
Qld	By default 200 penalty units ($26 110)
ACT	✓ 50 penalty units ($40 500)
NSW	✓ 500 penalty units ($55 000)
NT	By default 1250 penalty units ($193 750)

489 VLRC Report No 18 (2010) [6.83]–[6.87], Recs 19, 21.

490 See the discussion at [3.252]–[3.258] below.

491 AAUS and Liberty Victoria Paper (2015) [5.4].

492 See the legislation cited at n 483 above.

	Different penalty for a corporation
SA	✓ $75 000 (where device used in breach of the Act) or $50 000 (in other specified cases)
Tas	✓ 500 penalty units ($81 500)
Vic	✓ 1200 penalty units ($193 428)
WA	✓ $50 000

[3.232] The *Invasion of Privacy Act 1971* does not expressly provide for higher maximum penalties for corporations. However, a higher maximum penalty for corporations—of five times the prescribed maximum—applies by default pursuant to section 181B of the *Penalties and Sentences Act 1992*.[493]

[3.233] Accordingly, where the *Invasion of Privacy Act 1971* prescribes a maximum penalty of 40 penalty units ($5222) or two years imprisonment for breach of the use prohibition, the maximum penalty for a corporation is 200 penalty units ($26 110).

[3.234] This is less than the maximum penalty for corporations in other jurisdictions.[494]

[3.235] The *Invasion of Privacy Act 1971* makes express provision to ensure that, where a corporation has committed an offence under the Act, each executive officer of the corporation is liable for the same offence.[495]

[3.236] This applies to an executive officer—namely, a person who is 'concerned with, or takes part in, the corporation's management', whether or not the person is a director—if:[496]

> (a) the officer authorised or permitted the corporation's conduct constituting the offence; or
>
> (b) the officer was, directly or indirectly, knowingly concerned in the corporation's conduct.

493 Provision to similar effect applies in the Northern Territory under the *Interpretation Act* (NT) s 38DB.

494 It is also less than the fine that may be imposed on a corporation where an Act specifies a term of imprisonment as the only penalty for an offence. Section 181A of the *Penalties and Sentences Act 1992* (Qld) provides a scale of fines in this situation including a fine of up to 1660 penalty units ($216 713) if the imprisonment is more than one year but not more than two years, and an unlimited amount if the imprisonment is more than two years.

495 *Invasion of Privacy Act 1971* (Qld) s 49A. This applies in relation to offences against ss 43(1) (the use prohibition), 43(5) (breach of forfeiture order), 44(1), 45(1) (the communication or publication prohibitions) and 46(5) (breach of non-publication order). It does not matter whether the corporation has also been proceeded against for, or convicted of, the offence.

496 *Invasion of Privacy Act 1971* (Qld) s 49A(1).

[3.237] The section does not affect the liability of the corporation for the offence.[497]

[3.238] Similar provisions are included in many of the other jurisdictions, although their scope differs in some respects.[498] By way of example, the provisions in Tasmania and Western Australia exempt an officer from liability for the corporation's conduct if:[499]

- the corporation breached the relevant provision without the officer's knowledge;
- the officer was not in a position to influence the conduct of the corporation in relation to its breach; or
- the officer, being in such a position, used all due diligence to prevent the breach by the corporation.

[3.239] Ordinarily, a person should not be made responsible for acts or omissions over which they had no control. On the other hand, the individual liability of executive officers might encourage accountability and ensure that penalties for corporate breaches are not displaced, especially if the officer knew of the breach or was in a position to influence the corporation's conduct.[500]

Forfeiture orders

[3.240] In addition to criminal offences, the *Invasion of Privacy Act 1971* provides for the forfeiture of a listening device used in breach of the Act.

[3.241] If the court convicts a person of an offence against the use prohibition, the court may, by the conviction, order that the listening device be forfeited to the State and delivered by the person with possession of the device within the time and to the person specified in the order (a 'forfeiture order').[501]

[3.242] If the person does not comply, police are empowered to seize the listening device.[502]

[3.243] With the exception of Victoria, the surveillance devices legislation in the other Australian states and territories also provides for the court to make forfeiture

---

497 *Invasion of Privacy Act 1971* (Qld) s 49A(3)(a). Nor does it affect the liability of a person under the Criminal Code (Qld) ch 2 as a party to the offence: s 49A(3)(b).

498 See *Surveillance Devices Act 2007* (NSW) s 57; *Surveillance Devices Act* (NT) s 72; *Listening Devices Act 1991* (Tas) s 25; *Surveillance Devices Act 1999* (Vic) s 32A; *Surveillance Devices Act 1998* (WA) s 39. These provisions apply to a 'director' of the corporation, as well as to a person who is concerned in, or takes part in, the corporation's management.

499 *Listening Devices Act 1991* (Tas) s 25(1); *Surveillance Devices Act 1998* (WA) s 39(1). See also *Surveillance Devices Act* (NT) s 72(3); and *Surveillance Devices Act 1999* (Vic) s 32A(3) to generally similar effect.

500 See generally ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002) [8.6]–[8.12]; Office of Queensland Parliamentary Counsel, *Fundamental Legislative Principles: The OQPC Notebook* (2008) [2.9.10], [3.4.1]–[3.4.2].

501 *Invasion of Privacy Act 1971* (Qld) s 43(4). It is an offence, punishable on summary conviction by a fine of up to 20 penalty units ($2600), to contravene such an order: s 43(5).

502 *Invasion of Privacy Act 1971* (Qld) s 43(6).

orders upon conviction for an offence.[503] In some jurisdictions, the court may also order the forfeiture or destruction of the record made by the device.

[3.244] By way of example, the *Surveillance Devices Act* (NT) empowers the court, where a person is found guilty of an offence against the Act, to make additional orders for:[504]

- the forfeiture of the surveillance device (or connection device) used in connection with the offence; or
- the forfeiture of a report or record of information obtained by the use of the surveillance device.

[3.245] Before making such an order, the court may give notice to and hear the persons it considers appropriate.[505]

[3.246] Forfeiture orders are in addition to any penalty imposed for the offence.

Other prohibitions

[3.247] The surveillance devices legislation in some jurisdictions includes a small number of other ancillary prohibitions.[506]

[3.248] These include provisions that, variously, make it an offence to:

- possess a record of a private conversation knowing that it was obtained, directly or indirectly, from use of a surveillance device in breach of the legislation;[507]
- possess a surveillance device knowing that it is intended or mainly designed for use in breach of the legislation, or with the intention of using it, or it being used, in breach of the legislation;[508]

---

503 *Listening Devices Act 1992* (ACT) s 12; *Surveillance Devices Act 2007* (NSW) s 58; *Surveillance Devices Act* (NT) s 73; *Surveillance Devices Act 2016* (SA) s 40; *Listening Devices Act 1991* (Tas) s 26; *Surveillance Devices Act 1998* (WA) s 40.

Forfeiture orders are also provided for in the surveillance devices legislation in New Zealand, and in the telecommunications interception legislation in Canada: see *Crimes Act 1961* (NZ) s 216E; Criminal Code RSC 1985 c C-46, s 192.

504 *Surveillance Devices Act* (NT) s 73(1). A 'connection device' is defined in s 4 to mean 'a device that is not a surveillance device or part of a surveillance device but is ancillary to the installation, use, maintenance or retrieval of a surveillance device'.

505 *Surveillance Devices Act* (NT) s 73(2).

506 See, eg, [2.69] above. See also Appendix B.

507 See *Listening Devices Act 1992* (ACT) s 7; *Surveillance Devices Act 2007* (NSW) s 12; *Listening Devices Act 1991* (Tas) s 11; *Surveillance Devices Regulations 1999* (WA) reg 9. The prohibition does not apply where the person has possession of the record in connection with proceedings for an offence against the Act, with the consent of all the principal parties, or as a result of a communication or publication that does not breach the Act.

508 See *Listening Devices Act 1992* (ACT) s 8(a)(iv), (b); *Surveillance Devices Act 2007* (NSW) s 13(1)(c); *Surveillance Devices Act 1998* (WA) s 34. See also *Surveillance Devices Act 2016* (SA) s 36 which makes it an offence to possess a surveillance device of a declared class or kind without the Minister's consent; no devices have been declared.

- manufacture or supply, or offer to supply, a surveillance device knowing that it is intended or mainly designed for use in breach of the legislation, or with the intention of using it, or it being used, in breach of the legislation;[509] or
- advertise a listening device of a prescribed class or description.[510]

[3.249] These offences extend the reach of the legislation beyond those who use a surveillance device unlawfully. They would ensure, for example, that a person who possesses or supplies a surveillance device for the purpose of unlawful surveillance would also be in contravention of the legislation whether or not the surveillance occurs.[511] This might provide a further disincentive to unlawful surveillance.

[3.250] However, the diversity and ubiquity of many multi-purpose technologies that are capable of being used as surveillance devices—including smartphones and other smart devices and programs—may make it difficult to ensure that any prohibition on the possession, supply or advertising of such devices is both fair and practicable.

[3.251] The NZLC observed in this regard that it 'would be impossible to outlaw all devices that can be used to conduct unlawful surveillance', and that offences for making, selling or supplying a surveillance device or software would need to be 'very tightly drawn and restricted to cases in which a person is clearly aiding or encouraging the commission of a crime'. It observed, for example, that:[512]

> It [should] not be an offence to sell or supply a surveillance device if the person so doing did not know that the device was to be used to commit an offence under the Act. It [should], however, be an offence for a private investigator to supply a client with a tracking device, knowing that the client intended to install it in the car of his ex-partner for the purpose of tracking her.

[3.252] In Victoria, it has been suggested that the surveillance devices legislation should include an additional offence of a different kind, relating to harassment and intimidation.

[3.253] The VLRC recommended the creation of a new offence to make it unlawful to:[513]

---

509 See *Listening Devices Act 1992* (ACT) s 8(a)(i)–(iii), (b); *Surveillance Devices Act 2007* (NSW) s 13(1)(a)–(b), (2). This also includes sale or distribution.

510 See *Invasion of Privacy Act 1971* (Qld) s 48 (punishable on summary conviction by a fine of up to 20 penalty units ($2611) or imprisonment for one year). No devices have been prescribed for the purpose of this offence.

511 Under the Criminal Code (Qld) s 7 a person who enables, aids, counsels or procures another person to commit an offence is deemed to have taken part in committing the offence and to be guilty of the offence. In the context of 'aiding', however, something more than unwitting assistance would usually be required: see generally MJ Shanahan, SM Ryan and AJ Rafter, Lexis Advance, *Carter's Criminal Law of Qld* (September 2018) [s7.50].

512 NZLC Report No 113 (2010) [3.103]–[3.104]. The NZLC recommended that it should be an offence to make, sell or supply a surveillance device or software knowing that it is to be used to undertake surveillance in contravention of the criminal provisions of the surveillance devices legislation, or to promote or hold out a device or software as being useful for the carrying out of surveillance in contravention of the legislation: Rec 16.

513 VLRC Report No 18 (2010) Rec 20. See also Rec 21 as to the availability of both criminal and civil penalties for contravention of the proposed offence.

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.

[3.254] The VLRC explained that the 'primary purpose' of the offence would be 'to send a clear message to the community that various forms of behaviour with a surveillance device are unacceptable'. It referred, for example, to people filming acts of violence, the aftermath of traffic accidents or consensual sexual activities for 'entertainment', people being filmed while entering abortion clinics, gay bars or drug treatment clinics to intimidate them or hinder their passage, and to the potential use of surveillance for blackmail.[514]

[3.255] The VLRC observed that the protection offered by the surveillance devices legislation is generally limited to private conversations and activities. It observed that there are existing offences addressing matters such as stalking and offensive behaviour in public. However, in its view, a 'specific offence concerned with the grossly offensive use of a surveillance device' would provide a clearer message to the community.[515]

[3.256] A similar proposal was made by the AAUS and Liberty Victoria, observing that such an offence would focus on the harm caused by particular conduct.[516]

[3.257] In Queensland, there are a number of existing laws of general application that might apply to situations in which surveillance devices are used to intimidate, demean or harass. This includes Criminal Code offences dealing with unlawful stalking and observations or recordings in breach of privacy,[517] public nuisance offences under the *Summary Offences Act 2005*,[518] as well as the mechanisms for obtaining a domestic violence order under the *Domestic and Family Violence Protection Act 2012*.[519] There are also proposed new Criminal Code offences dealing with the distribution of images and recordings[520] and a proposal to introduce a

514 Ibid [6.96]–[6.101].

515 Ibid [6.105]–[6.106].

516 AAUS and Liberty Victoria Paper (2015) [4.5]. They proposed an offence in the same terms as the VLRC's recommended offence. They also proposed that there be a higher penalty where a person has contravened the use prohibition or the communication or publication prohibition and 'thereby cause[d] psychological or physical harm to another person'.

517 See Criminal Code (Qld) s 227A, ch 33A, discussed at [2.118] ff and [2.129] above. See also s 227B (distributing prohibited visual recordings).

518 See *Summary Offences Act 2005* (Qld) s 6. A public nuisance offence is committed if a person behaves in a disorderly, offensive, threatening or violent way, or if the person's behaviour interferes, or is likely to interfere, with the peaceful passage through or enjoyment of a public place by a member of the public: s 6(2). See also the *Police Powers and Responsibilities Act 2000* (Qld) ss 46, 47 as to police powers to give move on directions.

519 Examples of domestic violence include unauthorised surveillance and unlawful stalking: *Domestic and Family Violence Protection Act 2012* (Qld) s 8(2)(h)–(i). See generally QLRC, *Domestic Violence Disclosure Scheme*, Report No 75 (2017) [2.3]–[2.4], [3.14]–[3.45].

520 See the Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Bill 2018 (Qld), discussed at [2.123] ff above.

national 'right to be forgotten' law as part of a package of reforms to address cyberbullying.[521]

[3.258] Although not specific to the use of surveillance devices, such laws reflect general community expectations about the unacceptability of certain types of offensive conduct.

Civil remedies

[3.259] Penalties are generally designed to punish and deter wrongful conduct. In contrast, civil remedies are generally intended to compensate for the harm caused by the conduct to an individual. Whereas penalties are imposed by the State, civil remedies are traditionally pursued by the individual.[522]

[3.260] Civil remedies commonly include orders for monetary compensation (often called 'awards of damages'), orders to either restrain or require particular action (sometimes called 'injunctions'), and declarations (for example, about the lawfulness of a person's conduct).[523]

[3.261] Ordinarily, civil orders are enforceable through separate proceedings.[524] In some cases, the relevant legislation may also provide that breach of an order is a criminal offence—this applies, for example, to non-monetary orders of QCAT, peace and good behaviour orders and domestic and family violence orders.[525]

[3.262] For example, the *Domestic and Family Violence Protection Act 2012* provides a scheme for the court to make a civil protection order (called a 'domestic violence order') that imposes conditions on the respondent's conduct towards an aggrieved person. The order is made in civil proceedings, but breach of the order is a criminal offence.[526] In this way, the Act takes a staged approach to liability.

[3.263] The *Invasion of Privacy Act 1971* does not provide for any civil remedies for a breach of the Act. However, it includes the following saving provision:[527]

---

521 See Queensland Government, *Queensland Government Response to Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland* (October 2018) 13 in relation to Rec 29 of the report of the Queensland Anti-Cyberbullying Taskforce: see generally <https://campaigns.premiers.qld.gov.au/antibullying/taskforce/>.

522 See generally ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002) [2.15].

523 The types of remedies available depend on the jurisdiction and powers conferred on the court or tribunal: see, eg, *District Court of Queensland Act 1967* (Qld) pt 5 div 1; *Magistrates Act 1991* (Qld) s 8; *Justices Act 1886* (Qld) s 22A; *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 1.

524 See generally *Uniform Civil Procedure Rules 1999* (Qld) chs 19, 20. Non-compliance with a court or tribunal order might also be treated as a contempt of court: see, eg, *Magistrates Courts Act 1921* (Qld) s 50(1)(a).

525 See, respectively, the *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 213; *Peace and Good Behaviour Act 1982* (Qld) s 11; *Domestic and Family Violence Protection Act 2012* (Qld) s 177. See also, for example, the *Family Law Act 1975* (Cth) pt XIIIA which confers jurisdiction on the court to impose various sanctions for non-compliance with particular orders, including a fine or sentence of imprisonment.

526 See generally *Domestic and Family Violence Protection Act 2012* (Qld) pts 3, 5 div 1–2, s 177. Domestic violence orders are usually made by a magistrate or the Magistrates Court, but may also be made by a court that convicts a person of a domestic violence offence or by the Childrens Court: ss 6, 26, 32, 42, 43.

527 *Invasion of Privacy Act 1971* (Qld) s 51.

51 Saving of remedies

No proceedings or conviction for any offence against this Act shall affect any civil right or remedy to which any person aggrieved by the offence may be entitled.

[3.264] As discussed at [2.133] to [2.136] above, various civil remedies might be available to someone whose private conversations or activities have been the subject of surveillance, but these apply in a limited range of circumstances. The financial assistance scheme provided for in the *Victims of Crime Assistance Act 2009* is also limited in its application.[528]

[3.265] There are no civil remedy provisions in the surveillance devices legislation of the other Australian states and territories.

[3.266] However, specific provision for civil remedies is made in the *Telecommunications (Interception and Access) Act 1979* (Cth).

[3.267] As explained at [2.89] to [2.93] above, it is an offence under that Act to intercept a communication passing over a telecommunications system (section 7(1)) or to communicate, use or make a record of information obtained from such an interception (section 63).

[3.268] Part 2-10 of that Act provides that, where there has been a breach of those provisions, 'remedial relief' may be granted to an aggrieved person either:[529]

- by the court that convicts a person of an offence against section 7(1) or section 63, on application by the aggrieved person made as soon as practicable after the conviction; or
- by the Federal Court of Australia or a court of a State or Territory, on an application made by the aggrieved person within six years after the end of the interception or communication.

[3.269] A person is an aggrieved person 'if, and only if' the person was a party to the communication or the communication was made on the person's behalf.[530]

[3.270] The orders that may be made include:[531]

(a) an order declaring the interception or communication, as the case requires, to have been unlawful;

(b) an order that the defendant pay to the aggrieved person such damages as the court considers appropriate [including punitive damages];

---

528 The *Victims of Crime Assistance Act 2009* (Qld) is limited in its application to crimes involving violence, including domestic and family violence: see ss 25, 26, 27. An eligible primary victim may be granted up to $75 000 in assistance under that Act: s 38.

529 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 107A, 107B. Section 107A applies where an interception occurs in breach of s 7(1). It applies to communications in breach of s 63 if the information was obtained by an interception in breach of s 7(1).

530 *Telecommunications (Interception and Access) Act 1979* (Cth) s 107A(2).

531 *Telecommunications (Interception and Access) Act 1979* (Cth) s 107A(7), (9), (10).

> (c) an order in the nature of an injunction (including a mandatory injunction) [which may be varied or revoked];
>
> (d) an order that the defendant pay to the aggrieved person an amount not exceeding the amount that, in the opinion of the court, represents the total gross income derived by the defendant as a result of the interception or communication, as the case requires.

[3.271] This is not intended to be exhaustive, 'nor to fetter a court's discretion to order whatever remedy it thinks appropriate in the circumstances of each case'. The inclusion of punitive damages 'reflects the intention that this right of action act as a measure to enhance privacy'.[532]

[3.272] The civil remedies under that Act do not limit any liability (whether criminal or civil) that a person has under any other provision of the Act or under any other law.[533]

[3.273] Part 2-10 was added by the *Telecommunications (Interception) Amendment Act 1995* (Cth).[534] The amendments gave effect to the recommendations of a review into the long-term cost-effectiveness of telecommunications interception. Relevantly, the terms of reference required the review to consider:[535]

> Measures to safeguard individual privacy including … the effectiveness of Australia's present regulatory regime in protecting individual privacy from unlawful and unwarranted intrusion through telecommunications interception …

[3.274] The review found that the Act generally provided a high degree of privacy protection but that it could be enhanced by specific measures, including a right of action against a person who unlawfully intercepts or publishes a telecommunication.[536]

[3.275] It was observed that a civil right of action under the Act would fill a gap where prosecution of an offence may be unlikely, and would provide a 'more potent privacy protection'.[537]

[3.276] Provision for civil remedies is also made, in differing terms, in the telecommunications interception legislation in some other jurisdictions. For example,

---

532 Explanatory Notes, Telecommunications (Interception) Amendment Bill 1994 (Cth) 8.

533 *Telecommunications (Interception and Access) Act 1979* (Cth) s 107C(1).

534 *Telecommunications (Interception) Amendment Act 1995* (Cth) s 3, sch 1 pt 3 item 18. The civil remedy provisions were included 'to promote privacy': Explanatory Notes, Telecommunications (Interception) Amendment Bill 1994 (Cth) 2.

535 PJ Barrett, Commonwealth Department of Finance, 'Review of the Long Term Cost Effectiveness of Telecommunications Interception' (Report, March 1994) v, terms of reference para 3(e).

536 Ibid [4.3.6].

537 G Greenleaf, 'Interception of Communications—Australia: The Barrett Review—Part II' (1995) 11(4) *Computer Law & Security Review* 204, 205.

in Canada, the legislation empowers the court that convicts a person of a relevant offence to order up to $5000 in punitive damages to the aggrieved person.[538]

[3.277] In suggesting a similar approach for the interception legislation in New Zealand, the Privacy Commissioner of that jurisdiction expressed the view that:[539]

> civil remedies complete the appropriate range of safeguards in respect to interception of communications. … [Criminal offences] act as a deterrent and can punish wrongdoers who unlawfully intercept communications or who breach the statutory requirements for lawful interception. We have legal controls upon how lawful interceptions should be carried out … However, at the end of the day an individual whose private communications have been intercepted may be protected through civil remedies in a way that neither the criminal law nor administrative safeguards can achieve. An aggrieved individual has the greatest interest in his or her own privacy. Civil proceedings may also compensate an individual, something that neither criminal sanctions nor administrative admonitions can achieve.

[3.278] The ALRC noted that the surveillance devices legislation of the states and territories provides important privacy protections by creating offences for the unauthorised use of surveillance devices.[540] It considered that federal legislation should replace the existing state and territory statutes, and that it should empower a court to 'order remedial relief, including compensation, for a person subjected to unlawful surveillance'.[541] In making this recommendation, the ALRC explained that:[542]

> If surveillance legislation were enacted by the Commonwealth, there would be merit in both surveillance legislation and the [*Telecommunications (Interception and Access) Act 1979* (Cth)] providing similar options for compensation and redress.
>
> Criminal law generally punishes the offender without necessarily providing redress to the victim. While an individual who has been subjected to unlawful surveillance may gain some satisfaction from seeing the offender fined, and while the fine may dissuade the offender and others from conducting further unlawful surveillance in the future, the victim will generally not receive any compensation or other personal remedy.

[3.279] The ALRC observed that an approach similar to that taken under the *Telecommunications (Interception) Amendment Act 1995* (Cth) would provide a 'quicker, cheaper and easier means of redress' than a general statutory tort for

538 Criminal Code RSC 1985 c C-46, s 194. The federal wiretap and electronic communications privacy legislation in the United States of America also provides for remedial relief, including damages, in a civil action by a person whose wire, oral or electronic communication is intercepted, disclosed or intentionally used in violation of ch 119: 18 USCA § 2520.

539 Privacy Commissioner of New Zealand, 'Interception of Private Communications' (Report, April 1997) [4.8.2].

540 See ALRC Report No 123 (2014) ch 14.

541 Ibid Recs 14-1, 14-7.

542 Ibid [14.86]–[14.87].

serious invasions of privacy because it would not require the individual to pursue separate civil proceedings in addition to the prosecution for the offence.[543]

[3.280] The ALRC also observed that, although statutory compensation schemes for victims of crime exist in the states and territories, those schemes 'are generally only available for serious physical crimes such as assault, robbery, or sexual assault, and surveillance is therefore unlikely to give rise to compensation under these schemes'.[544]

[3.281] Others have similarly recommended that surveillance devices legislation should provide for civil remedies. For example, the recent review of the legislation in the Australian Capital Territory recommended that:[545]

> consideration [should] be given to expanding the range of remedial options available for contravention of the Surveillance Act, including allowing access to the ACT Civil and Administrative Tribunal to seek monetary compensation.

[3.282] That report observed that alternative reform options, such as extending the ambit of the information privacy legislation or establishing a tort for serious invasions of privacy would 'have implications beyond surveillance' and as such 'are beyond the scope' of that review.[546]

[3.283] The NZLC took a similar approach, recommending that surveillance devices legislation should include a civil right of action with standard civil remedies being available if it is proved, to the civil standard, that one of the criminal provisions of the Act has been breached.[547]

[3.284] The NSWLRC proposed a regulatory framework for surveillance under which breaches of the legislation would give rise to civil liability. In addition to a complaints mechanism to the Privacy Commissioner, it recommended that the Administrative Decisions Tribunal should have wide powers to grant relief in proceedings brought by an affected person, including damages of up to $150 000, orders to prevent the continuation or repetition of the conduct, 'mandatory' orders (for example, for the removal of surveillance devices or the destruction of surveillance material), declarations that certain conduct is unlawful, orders for the publication of apologies and non-disclosure orders.[548]

---

543 Ibid [14.88]. A number of reviews have recommended, proposed or considered the introduction of a general statutory 'tort' or cause of action for serious invasions of privacy, but none has been enacted: see, eg, ALRC Report No 123 (2014) pt 2; Australian Government Issues Paper: Serious Invasion of Privacy (2011) 16 ff; Eyes in the Sky Report (2014) Rec 3; Eyes in the Sky Report: Government Response (2016) 8; NSWLRC Report No 120 (2009); NSW Parliamentary Committee Report (2016) Rec 3; VLRC Report No 18 (2010) Recs 22–24.

544 ALRC Report No 123 (2014) [14.89].

545 ACT Review (2016) [2.5](j), [6.47].

546 Ibid [7.1]–[7.2].

547 NZLC Report No 113 (2010) [3.105], Rec 17.

548 NSWLRC Interim Report No 98 (2001) [10.6], Rec 112. The 'Administrative Decisions Tribunal' has since been replaced in New South Wales with the 'Civil and Administrative Tribunal'. As to the complaints mechanism to the Privacy Commissioner, see [3.299]–[3.300] below.

[3.285] A similar proposal was made by the AAUS and Liberty Victoria.[549]

Questions

Q-21 Should prohibited use of a surveillance device or prohibited communication or publication of information obtained through the use of a surveillance device be punishable:

(a) as a criminal offence; or

(b) by a civil penalty; or

(c) as either a criminal offence or a civil penalty, as alternatives?

Q-22 How should the liability of a corporation, or a corporate officer, for a contravention by the corporation be dealt with?

Q-23 Should there be power to order the forfeiture of a surveillance device used in a contravention of the legislation, or of a report or record of information obtained by the use of a surveillance device in a contravention of the legislation?

Q-24 Is it necessary for the legislation to include any other ancillary prohibitions, for example, to deal with:

(a) the possession of records obtained from the prohibited use of surveillance devices?

(a) the possession, manufacture, supply or advertising of surveillance devices?

(b) the use of surveillance devices to intimidate, harass or hinder a person?

Q-25 Should there be a right to bring a civil proceeding in respect of a contravention of the prohibited use of a surveillance device or the prohibited communication or publication of information obtained through the use of a surveillance device?

Q-26 If yes to Q-25, what relief should be available to a plaintiff in a civil proceeding, for example:

(a) an order that the contravener is prohibited from conduct (for example, from using a surveillance device) or must do something (for example, remove a surveillance device)?

549 AAUS and Liberty Victoria Paper (2015) [5.3]. They proposed that the relevant civil and administrative tribunal of the state or territory be empowered, in hearing complaints about breaches of the legislation, to make orders to restrain the respondent from continuing or repeating the conduct, for the respondent to take steps to redress the loss or damage, or for the respondent to pay compensation of up to $100 000, and to make a declaration that the person's privacy has been breached by the prohibited conduct.

(b) a declaration (that the conduct was unlawful or that the unlawful conduct breached the person's privacy)?

(c) an order for monetary compensation (for any loss or damage or up to any particular amount)?

(d) other relief?

Q-27 If yes to Q-26(a), should breach of a prohibitory or mandatory order be a criminal offence or dealt with as a contempt or by some other procedure?

Enforcement and regulatory powers

Police and prosecution

[3.286] The regulatory and compliance mechanism of the *Invasion of Privacy Act 1971* is primarily criminal, relying on police investigation and prosecution of offences.

[3.287] The position is similar in the other jurisdictions. In two jurisdictions, the surveillance devices legislation expressly requires the consent of either the Attorney General[550] or the Director of Public Prosecutions[551] to institute proceedings for an offence.

[3.288] This approach focuses on enforcement of criminal breaches and is likely to be reserved for more serious cases where there is clear evidence of offending.[552] It might not represent a practical avenue for ongoing compliance monitoring or for dealing with more minor or common complaints and disputes.

Independent regulator

[3.289] A feature of some regulatory regimes that aim to support best practices in industry or agency dealings with members of the community is an independent regulator with specified oversight functions and powers. This applies, for example, under the *Privacy Act 1988* (Cth), the IP Act and the *Anti-Discrimination Act 1991*.

[3.290] Reviews in some other jurisdictions have proposed that surveillance devices legislation should also have an independent regulator.[553]

[3.291] This could provide a lower cost and less formal avenue for dealing with possible breaches, or an avenue for research, public awareness, expert advice and guidance. On the other hand, the introduction of an independent regulator would involve additional costs, with a potential increase in regulatory burden.

[3.292] It has been suggested that the functions of existing 'Privacy Commissions' under information privacy legislation could be extended to cover new functions under surveillance devices legislation.[554]

[3.293] For example, in its review of surveillance in public places, the VLRC explained that:[555]

---

550 *Surveillance Devices Act 2007* (NSW) s 56.

551 *Listening Devices Act 1991* (Tas) s 24.

552 See generally Office of the Director of Public Prosecutions, *Director's Guidelines* (30 June 2016) [4] at <https://www.justice.qld.gov.au/corporate/justice-agencies/office-of-the-director-of-public-prosecutions> which explain that 'the prosecution process should be initiated or continued wherever it appears to be in the public interest'.

553 See NSWLRC Interim Report No 98 (2001) [4.67]–[4.73], [10.29]–[10.35], Recs 91, 92; NSWLRC Report No 108 (2005) [4.36]–[4.37], Rec 2; VLRC Report No 18 (2010) [5.31] ff, Recs 3 to 9; NZLC Report No 113 (2010) [4.6]–[4.8] Rec 18. See also AAUS and Liberty Victoria Paper (2015) [1.2](8), [5].

554 See NSWLRC Interim Report No 98 (2001) [4.67]; NSWLRC Report No 108 (2005) Rec 2; VLRC Report No 18 (2010) Rec 9; NZLC Report No 113 (2010) Rec 18.

555 VLRC Report No 18 (2010) [5.99]–[5.100]. See also AAUS and Liberty Victoria Paper (2015) [5].

> The commission believes it is more appropriate to extend the functions of an existing regulator to regulate surveillance in public places than to create a new regulator. This approach is consistent with the Victorian Government's commitment to devise regulatory options that are as cost-effective as possible and that minimise the regulatory burden on agencies and organisations.
>
> … the Victorian Privacy Commissioner appear[s] to be an obvious choice to exercise regulatory functions in relation to public place surveillance because of the Commissioner's expertise in protecting privacy.

[3.294] In Queensland, the Information Commissioner, supported by the Privacy Commissioner, has a range of functions under the IP Act, including management and mediation of privacy complaints against Queensland government agencies, monitoring and reporting on agency compliance, and education and training.[556]

[3.295] As explained at [2.104] above, the IP Act applies only to personal information handled by Queensland government agencies. Accordingly, it presently has a limited application to surveillance activities. The Information Commissioner has released guidelines under the IP Act for government agencies about privacy and the use of camera surveillance or drones.[557]

[3.296] The Human Rights Bill 2018—which provides for a right to 'privacy and reputation'[558]—proposes to rename the Anti-Discrimination Commission Queensland as the Queensland Human Rights Commission ('QHRC') and to confer on it additional oversight functions and powers under the Bill.[559]

[3.297] As such, the proposed QHRC could be expected to develop a relevant expertise in dealing with privacy infringements. Like the IP Act, however, the Bill generally applies only to the activities of public entities.

Complaints mechanism

[3.298] None of the Australian jurisdictions includes a specific complaints mechanism in their surveillance devices legislation, but this has been proposed in some jurisdictions.

[3.299] For example, the NSWLRC recommended that complaints about breaches of the surveillance devices legislation should be made to the Privacy Commissioner in that jurisdiction for conciliation and, if unresolved, referred to the Administrative Decisions Tribunal for decision. It also considered that the Privacy Commissioner

---

556 See generally *Information Privacy Act 2009* (Qld) ch 4; Office of the Information Commissioner Queensland, *Key functions* (2018) <https://www.oic.qld.gov.au/about/our-organisation/key-functions>. The Information Commissioner is established under the *Right to Information Act 2009* (Qld) ch 4.

557 See [2.111] above, [C.19]–[C.20] below.

558 Human Rights Bill 2018 (Qld) cl 25. However, the Bill also provides that, if the subject of a complaint could be the subject of a privacy complaint under the IP Act, the Human Rights Commissioner may refer the complaint to the Information Commissioner: cl 73(4). See also [2.100]–[2.102] above.

559 Human Rights Bill 2018 (Qld) pts 4, 7 div 2.

should have power to conduct inquiries and initiate investigations into breaches or threatened breaches of the legislation.[560]

[3.300] In making its recommendations—which were modelled on the complaints processes of other legislation—the NSWLRC observed that:[561]

> The benefits of providing access to conciliation in the first instance, and determination by [the tribunal] in the second instance, are several. The conciliation process is:
>
> - readily accessible by complainants;
> - relatively inexpensive;
> - not intimidating; and
> - can bring flexibility and informality to bear on the resolution of complaints.
>
> Furthermore, a Privacy Commissioner would obviously develop specialist skill and expertise in conciliating breaches of the proposed Surveillance Act.

[3.301] A similar approach was proposed by the AAUS and Liberty Victoria.[562]

[3.302] In Queensland, like New South Wales, the *Anti-Discrimination Act 1991* (as well as the Human Rights Bill 2018) provides for complaints about breaches of the legislation to be made to the Commissioner for conciliation.[563] Conciliation is also a feature of some other legislative schemes, including the *Privacy Act 1988* (Cth).[564]

[3.303] Conciliation, which is a form of alternative dispute resolution, usually involves a third party acting in an advisory role to facilitate an agreed resolution of a dispute with reference to the relevant legal principles. It generally aims to provide for a less formal and faster resolution of disputes.[565]

[3.304] In contrast, the IP Act provides for the Information Commissioner to deal with privacy complaints by mediation, or referral to the Queensland Civil and Administrative Tribunal ('QCAT') for determination.[566] Mediation is similar to

---

560 See NSWLRC Interim Report No 98 (2001) Recs 91–102, 105. It also recommended that the Privacy Commissioner should have standing to bring (including in a representative capacity) or intervene in tribunal proceedings. As to the proposed powers of the tribunal, see [3.284] above. The 'Administrative Decisions Tribunal' has since been replaced in New South Wales with the 'Civil and Administrative Tribunal'.

561 Ibid [10.29]–[10.30]. The recommendations were modelled on the processes under the *Anti-Discrimination Act 1977* (NSW) and the *Privacy and Personal Information Protection Act 1998* (NSW).

562 AAUS and Liberty Victoria Paper (2015) [5.1]–[5.2].

563 *Anti-Discrimination Act 1991* (Qld) ch 7 pt 1 div 3; Human Rights Bill 2018 (Qld) pt 4 div 2 subdiv 4.

564 *Privacy Act 1988* (Cth) s 40A. See also, eg, *Australian Human Rights Commission Act 1986* (Cth) pt IIB div 1; *My Health Records Act 2012* (Cth) s 73(3)(a); *Health Ombudsman Act 2013* (Qld) pt 11; *Residential Tenancies and Rooming Accommodation Act 2008* (Qld) ch 6 pt 1; *Industrial Relations Act 2016* (Qld) ch 4 pt 3 div 1.

565 See, eg, Human Rights Bill 2018 (Qld) cl 80. Conciliation is often distinguished from mediation in that the conciliator plays a more direct, advisory role: see [3.304] and n 567 below.

566 *Information Privacy Act 2009* (Qld) ch 5 pts 3, 4.

conciliation but generally involves the third party taking a less advisory and more facilitative role.[567]

[3.305] The ALRC, which recommended the inclusion of a civil right of action under surveillance devices legislation, also recommended a complaints mechanism for surveillance disputes between residential neighbours. It explained that:[568]

> A number of submissions to [the ALRC's] Inquiry have raised concerns regarding CCTV cameras, installed for security in homes and offices that may also record the activities of neighbours. A low cost option for resolving disputes about surveillance devices is desirable, particularly where prosecution under surveillance legislation is inappropriate, undesirable or unsuccessful.

[3.306] Rather than making complaints to an independent regulator, the ALRC suggested that jurisdiction be given to 'appropriate courts and tribunals', such as civil and administrative tribunals like QCAT or specialist courts like the Queensland Planning and Environment Court. It observed that:[569]

> Many of the types of disputes that may currently be heard in these tribunals involve an element of privacy, and in particular the protection of privacy in disputes between neighbours. … In *des Forges v Kangaroo Point Residents Association*, the [Queensland Planning and Environment Court] set aside development approval for three residential towers because 'insufficient regard has been paid to the actual intensity of the development, to boundary clearances, separation, privacy and the consequential effects on views'. (note omitted)

[3.307] In Queensland, some specific neighbour disputes are also dealt with under the *Neighbourhood Disputes (Dividing Fences and Trees) Act 2011*.[570]

Inspections

[3.308] Some regulatory regimes include inspection powers to aid in monitoring or investigating compliance with relevant legislation.[571]

[3.309] The *Invasion of Privacy Act 1971* includes provisions for the appointment of 'inspectors',[572] but these provisions no longer appear to be used.[573]

---

567 See generally NADRAC, *Your Guide to Dispute Resolution* (Australian Government, Attorney-General's Department, 2012) at <https://www.ag.gov.au/LegalSystem/AlternateDisputeResolution/Pages/default.aspx>.

568 ALRC Report No 123 (2014) Rec 14-8, [14.90]. See [3.278]–[3.280] above as to the ALRC's recommendation for a civil right of action.

569 Ibid [14.91]–[14.92], citing *des Forges v Kangaroo Point Residents Association* [2001] QPEC 061 (Judge Brabazon QC).

570 The *Neighbourhood Disputes (Dividing Fences and Trees) Act 2011* (Qld) confers jurisdiction on QCAT to hear disputes about dividing fences and trees in particular circumstances: see generally QLRC, *Review of the Neighbourhood Disputes (Dividing Fences and Trees) Act 2011*, Report No 72 (2015) [4.141] ff.

571 See, eg, *National Measurement Act 1960* (Cth) pt IX; *Casino Control Act 1982* (Qld) pt 9; *Fair Trading Inspectors Act 2014* (Qld); *Fisheries Act 1994* (Qld) pt 8 divs 1–2, 4.

572 *Invasion of Privacy Act 1971* (Qld) pt 2.

573 Information provided by the Office of Fair Trading, Department of Justice and Attorney-General (Queensland), 15 November 2018. Inspectors have not been appointed under the *Invasion of Privacy Act 1971* (Qld) since at least 2006.

[3.310] The provisions for inspectors were included when the Act was first introduced; at that time, the Act also dealt with the control of credit reporting agents and private inquiry agents. Those matters are now regulated under different legislation.[574]

[3.311] The Act continues to provide that inspectors may be appointed who may 'at any time do any or all of the following':[575]

> (a) make such examination and inquiry as may be necessary to ascertain whether the provisions of this Act have been or are being complied with and interrogate any person for that purpose …;
>
> (b) enter any premises at the registered address of any licensee and inspect and examine any books and papers found upon such entry;
>
> (c) call to his or her aid any person whom the inspector may think competent to assist him or her in the exercise of any power aforesaid;
>
> (d) exercise such other powers as may be prescribed.

[3.312] Inspection provisions apply to surveillance by law enforcement agencies,[576] but are not otherwise included in the surveillance devices legislation of other jurisdictions.

[3.313] The NSWLRC recommended that the Privacy Commissioner's functions and powers should be extended under the surveillance devices legislation to include:[577]

- appointing inspectors to investigate complaints, and to conduct both routine and random inspections of surveillance systems or devices to ascertain compliance with the proposed Act;
- right of entry to non-residential premises to inspect surveillance systems or devices to ascertain compliance with the proposed Act.

[3.314] This would apply to overt surveillance activities, such as the use of security cameras in public places or business premises.[578] The NSWLRC explained that the inspection powers would allow the Privacy Commissioner in that jurisdiction to

---

574 See, respectively, *Privacy Act 1988* (Cth) pt IIIA; *Security Providers Act 1993* (Qld). See also *Fair Trading Inspectors Act 2014* (Qld) which applies to inspections under the *Security Providers Act 1993* (Qld).

Former pt 3 of the *Invasion of Privacy Act 1971* (Qld), which dealt with credit reporting and private inquiry agents, was amended by the *Security Providers Act 1993* (Qld) ss 63–84 (Act as passed), and then omitted by the *Tourism, Racing and Fair Trading (Miscellaneous Provisions) Act 2002* (Qld) s 45.

575 *Invasion of Privacy Act 1971* (Qld) s 7(1). The privilege against self-incrimination is expressly preserved: s 7(2). 'Licensee', in s 7(1)(b), is not defined in the Act. No additional powers are prescribed under s 7(2)(d).

576 In Queensland, see *Police Powers and Responsibilities Act 2000* (Qld) ch 13 pt 5 div 3. In other jurisdictions see, eg, *Surveillance Devices Act 2007* (NSW) pt 5 div 3. These provisions relate to inspections of the records of law enforcement agencies and related reporting requirements.

577 NSWLRC Report No 108 (2005) Rec 2.

578 Ibid. The recommendation applies to 'overt' surveillance, but not to 'covert' surveillance which the NSWLRC proposed to regulate differently: see generally [D.2] ff below.

observe the operation of surveillance systems and ascertain whether those operations comply with the legislation.[579]

Enforcement powers

[3.315] Regulatory regimes also sometimes confer specific enforcement powers on particular entities.

[3.316] As noted at [3.229] above, the VLRC recommended the inclusion of civil penalties, as an alternative to criminal penalties, in the surveillance devices legislation. It recommended that the Privacy Commissioner should be given additional functions and powers under the legislation to investigate potential breaches and, where appropriate, to institute civil penalty proceedings in the Victorian Civil and Administrative Tribunal ('VCAT').[580]

[3.317] In their view, this would provide a greater range of regulatory measures to control the use of surveillance, and would be consistent with other legislation, including the *Privacy Act 1988* (Cth) and the *Competition and Consumer Act 2010* (Cth).[581]

[3.318] For example, under the *Privacy Act 1988* (Cth), the Information Commissioner has power to investigate acts or practices that may be an interference with the privacy of an individual or a breach of APP 1, and to apply to the Federal Court or Federal Circuit Court for civil penalty orders.[582]

[3.319] In Queensland, the IP Act takes a different approach. It empowers the Information Commissioner to conduct reviews into the personal information handling practices of relevant entities, and to issue 'compliance notices' to require an agency to take stated action within a particular time.[583] A compliance notice may be issued if:[584]

> the commissioner is satisfied on reasonable grounds that the agency—
>
> (a) has done an act or engaged in a practice in contravention of the agency's obligation to comply with the privacy principles; and
>
> (b) the act or practice—
>
> (i) is a serious or flagrant contravention of the obligation; or
>
> (ii) is of a kind that has been done or engaged in by the agency on at least 5 separate occasions within the last 2 years.

---

579 NSWLRC Interim Report No 98 (2001) [4.70].

580 VLRC Report No 18 (2010) Recs 4(g), 9, [5.95].

581 Ibid [5.95], [5.97]–[5.98], referring to the *Trade Practices Act 1974* (Cth), now the *Competition and Consumer Act 2010* (Cth).

582 See *Privacy Act 1988* (Cth) ss 40(2), 80U; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) pt 4.

583 *Information Privacy Act 2009* (Qld) s 135(1)(a)(i), ch 4 pt 6.

584 *Information Privacy Act 2009* (Qld) s 158(1). Failure to comply with a compliance notice is an offence punishable by up to 100 penalty units ($13 055): s 160.

Education and reporting

[3.320] Independent regulators often have more general roles in promoting compliance, offering guidance and informing the public about relevant issues.[585]

[3.321] The VLRC considered that this should be the primary function of an independent regulator for public place surveillance:[586]

> The commission believes there should be an independent regulator to guide responsible use of public place surveillance in Victoria. The primary roles of the regulator would be to promote the responsible use of surveillance in public places by providing practical guidance to surveillance users, and to keep the government and the people of Victoria fully informed of rapidly changing technology.
>
> …
>
> Surveillance users should be encouraged to work with a regulator to ensure that they are conducting surveillance responsibly and in accordance with public place surveillance guidelines.

[3.322] In particular, it recommended that the Privacy Commissioner should be responsible for:[587]

- research and monitoring, including use [of] technologies and current laws
- educating, providing advice and promoting understanding of laws and best practice
- developing and publishing best practice guidelines
- reviewing advice prepared by public authorities and significant private users of public place surveillance
- examining the practices of public authorities and significant private users in relation to their public place surveillance practices
- advising a public authority or significant private organisation of any failure to comply with laws and best practice guidelines

  … [and]

- reporting to the Minister on an annual basis on any matters in relation to any of its functions, including any failure by public authorities and significant organisations to comply with advice …

[3.323] The VLRC considered that this approach would ensure better understanding and awareness about the nature and extent of surveillance, address the need for practical guidance about how to conduct surveillance responsibly, inform

585 See also [2.110]–[2.111] above, [C.19]–[C.20] below.

586 VLRC Report No 18 (2010) [5.31]–[5.34].

587 Ibid Recs 4(a)–(f), (h), 9; and see [5.41] ff.

members of the public about their rights if surveillance is misused, and provide valuable information to legislators.[588]

[3.324] Subsequently to the VLRC's report, a number of guidelines about the use of CCTV and other surveillance in public places or by the public sector have been released by the Victorian Information Commissioner and other bodies.[589] The guidelines cover a range of matters, including that:

- the installation of CCTV should be guided by clear processes and based upon an assessment of relevant factors (such as the necessity for and purpose of the CCTV, its likely effectiveness, available alternatives, community and stakeholder consultation, and the impact on privacy);
- users of CCTV should have clear policies that address matters such as:
  - the installation, purpose and objectives of the use of CCTV;
  - the collection and security of data, and record-keeping and disposal;
  - management of the misuse of a CCTV system or related data, or a breach of policies about surveillance; and
  - privacy considerations;
- policies should be supported by operating procedures manuals, including technical information and matters relevant to daily management and use; and
- users of CCTV should take reasonable steps to inform people of surveillance (for example, people should be provided with notice that CCTV is being used, as well as the name and contact details of the user and guidance for how they can obtain further information).

[3.325] The NSWLRC similarly recommended that the Privacy Commissioner in that jurisdiction be empowered under the surveillance devices legislation to:[590]

- promote and provide assistance for compliance with the 'surveillance principles';
- assist surveillance users in drafting codes of practice; and

---

588 See generally VLRC Report No 18 (2010) [5.46] ff.

589 See Victorian Ombudsman, *Closed Circuit Television in Public Places—Guidelines: Victorian Ombudsman's Guidelines for Developing Closed Circuit Television Policies for Victorian Public Sector Bodies* (November 2012); Office of the Victorian Information Commissioner (formerly Commissioner for Privacy and Data Protection), *Guidelines to Surveillance and Privacy in the Victorian Public Sector* (May 2017); Victoria State Government, *Guide to Developing CCTV for Public Safety in Victoria: A Community Crime Prevention Initiative* (June 2018).

See also Victorian Auditor-General's Office, *Security and Privacy of Surveillance Technologies in Public Places*, Independent Assurance Report to Parliament 2018–19 No 9 (September 2018) [1.3] and fig 1B in the context of guidance to councils on the use and oversight of surveillance technology to protect privacy and data security.

590 NSWLRC Report No 108 (2005) Rec 2. The NSWLRC recommended a set of surveillance principles to govern the conduct of overt surveillance: see generally [D.6] below.

- educate the public on the acceptable use of surveillance devices.

[3.326] The NZLC particularly focused on the role of an independent regulator in reporting on developments to Parliament. It considered that:[591]

> we think it would be a good idea if the Privacy Act empowered the Privacy Commissioner to report regularly (perhaps every year, or every two years) to Parliament on developments in surveillance and surveillance technologies, and their implications for New Zealand. This would ensure that an independent agency is monitoring the growing potential of surveillance, and regularly bringing issues concerning surveillance to public attention. As part of this reporting function, the Privacy Commissioner could report on the operation and effectiveness of the Surveillance Devices Act, and on whether any amendments to the Act are required as a result of technological developments or other factors.

[3.327] At present in Queensland, the Information Commissioner has specific 'performance monitoring and support' functions under the IP Act, including promoting understanding of and compliance with the IPPs, providing best practice advice and assistance, initiating privacy education and training, issuing guidelines on privacy best practice, and reporting on reviews to the Speaker of the Legislative Assembly.[592]

[3.328] Similar education and advice functions are conferred on the Anti-Discrimination Commission under the *Anti-Discrimination Act 1991* and are proposed to be conferred on the QHRC by the Human Rights Bill 2018.[593]

Questions

Q-28 Should there be an independent regulator and, if so, what entity should this be?

Q-29 What regulatory and compliance functions or powers should be conferred on an independent regulator or otherwise provided for under the legislation, for example:

(a) conciliation or mediation of complaints about breaches of the legislation;

(b) appointment of inspectors to investigate or monitor compliance with the legislation;

(c) the issue of compliance notices;

(d) starting civil penalty proceedings;

(e) education and best practice guidance and advice about the legislation;

591 NZLC Report No 113 (2010) [4.7].

592 See *Information Privacy Act 2009* (Qld) s 135(1). See also [2.110]–[2.111] above, [C.19]–[C.20] below.

593 See *Anti-Discrimination Act 1991* (Qld) s 235(d), (e), (i); Human Rights Bill 2018 (Qld) cl 61(c)–(f).

(f) research, monitoring and reporting of matters relevant to the legislation?

Appendix A

Terms of reference

Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies

Background

With the advent of readily available technologies, including smartphones, drones fitted with cameras, and tracking and data surveillance devices, governments are increasingly expected to protect individuals from unreasonable intrusions on their privacy.

The need to regulate the use of surveillance devices and technologies to protect individuals against interferences with their privacy must be balanced against the legitimate uses of surveillance.

Queensland's *Invasion of Privacy Act 1971* provides a number of offences relating to the use of listening devices to overhear, record, monitor or listen to private conversations. However, the *Invasion of Privacy Act 1971* does not prohibit or regulate optical, tracking or data surveillance devices.

As a result, Queenslanders must rely on general laws where surveillance devices have unreasonably intruded on their privacy. These laws include common law actions such as trespass and nuisance, the *Invasion of Privacy Act 1971* in limited circumstances and section 227A of the *Criminal Code Act 1899* (which prohibits a person observing or visually recording another person in circumstances where a reasonable adult would expect to be afforded privacy without that person's consent).

In most other States and the Northern Territory, surveillance device legislation applies and extends beyond regulating the use of listening devices.

Concerns regarding the adequacy of Queensland's legislation to protect the privacy of individuals with the emergence of new technology are noted in the Queensland Drones Strategy released in June 2018. A key action item in the Queensland Drones Strategy is for the Queensland Government to refer to the Queensland Law Reform Commission (Commission) the question of whether Queensland's legislation adequately protects the privacy of individuals in the context of modern and emerging technologies.

Queensland law already regulates the use of surveillance devices by law enforcement agencies—for example, surveillance conducted pursuant to a warrant or emergency authorisation under the *Police Powers and Responsibilities Act 2000*. The review is not intended to extend to such provisions in existing legislation.

Terms of Reference

I, YVETTE MAREE D'ATH, Attorney-General, Minister for Justice and Leader of the House, refer to the Commission for review and investigation, the issue of modernising Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies pursuant to section 10 of the *Law Reform Commission Act 1968*.

Scope

The Commission is asked to recommend whether Queensland should consider legislation to appropriately protect the privacy of individuals in the context of civil surveillance technologies, including to:

1. regulate the use of surveillance devices (such as listening devices, optical surveillance devices, tracking devices and data surveillance devices) and the use of emerging surveillance device technologies (including remotely piloted aircraft (or 'drones') fitted with surveillance devices) to appropriately protect the privacy of individuals;

2. regulate the communication or publication of information derived from surveillance devices;

3. provide for offences relating to the unlawful use of surveillance devices and the unlawful communication or publication of information derived from a surveillance device;

4. provide appropriate regulatory powers and enforcement mechanisms in relation to the use of surveillance devices;

5. provide appropriate penalties and remedies; and

6. otherwise appropriately protect the privacy of individuals in relation to the use of surveillance devices.

In making its recommendations, the Commission should have regard to the following:

A. legislative and regulatory arrangements in Queensland, Australian and international jurisdictions, including permissible uses of surveillance devices;

B. law reform and parliamentary inquiry reports in other Australian jurisdictions;

C. the views expressed to the Commission following consultation with stakeholders, including with the community, academics and specialists in privacy law;

D. enforcement issues that are likely to arise from any new provisions, including what, if any, additional regulatory or other powers might be required, how provisions will be enforced, and whether any particular authority is best placed to do so;

E. Queensland's existing law regulating the use of surveillance devices for state law enforcement purposes is excluded from the review;

F. the issue of whether there should be a legislative framework to regulate the surveillance of workers by employers using surveillance devices (such as optical surveillance devices, tracking devices, listening devices and data surveillance devices) is excluded from this review; and

G. any other practical issues likely to arise.

The Queensland Law Reform Commission is asked to prepare draft legislation based on its recommendations.[594]

Consultation

The Commission shall consult with any group or individual, in or outside of Queensland, to the extent that it considers necessary.

Timeframe

The Commission is to provide a report on the outcomes of the review to the Attorney-General and Minister for Justice and Leader of the House by ~~**1 July 2019**~~ **31 October 2019**.[595]

Dated the 24th day of July 2018

YVETTE D'ATH MP
Attorney-General and Minister for Justice
Leader of the House

---

594 This amendment to the terms of reference, was made by a letter from the Attorney-General and Minister for Justice, Leader of the House, the Hon Yvette D'Ath MP, to the Chair of the Queensland Law Reform Commission, the Hon Justice David Jackson, dated 7 December 2018.

595 Ibid.

Appendix B

Comparative table of Australian legislation

[B.1] The table on the following pages provides an overview of relevant legislation in Australia, including surveillance devices legislation[596] and the *Telecommunications (Interception and Access) Act 1979* (Cth). It should be read together with the discussion in the body of this paper.

[B.2] The table includes information about offences under the 'use prohibition' and the 'communication or publication prohibitions'. It includes information about consent as an exception to the prohibitions, but does not provide a comprehensive overview of other exceptions. For a summary of all of the exceptions, see the discussion in Part 3 of this paper.

596 *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *Invasion of Privacy Act 1971* (Qld); *Surveillance Devices Act 2016* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).

	ACT	NSW	NT	QLD	SA
USE PROHIBITION OFFENCES					
Listening device: use, install or maintain a listening device to listen to or record a private conversation	✓ (without consent)	✓ (without consent)	✓ (without consent where person is not a party; but not an offence where person is a party)	✓ (unless person is a party)	✓ (without consent)
Optical surveillance device: use, install or maintain an optical surveillance device to observe or record a private activity		✓ (on or within premises, vehicle or object, if it involves entry or interference without consent; applies to any activity)	✓ (without consent where person is not a party; but not an offence where person is a party)		✓ (on or in premises, vehicle or any other thing without consent of each party, and without consent for any entry or interference)
Tracking device: use, install or maintain a tracking device to determine or monitor the geographical location of a person or an object		✓ (without consent)	✓ (without consent)		✓ (without consent)
Data surveillance device: use, install or maintain a data surveillance device to monitor or record information input into or output from a computer		✓ (by any person; on or in premises, if involves entry or interference without consent)	✓ (by law enforcement officer; without consent of person on whose behalf information is being input or output)		✓ (by any person; without consent of owner, or person in lawful control or management, of computer)
Telephone communication: intercept (including listen to or record) a telephone communication					
COMMUNICATION OR PUBLICATION PROHIBITION OFFENCES					
Party: communicate or publish record of conversation	✓ (without consent)			✓ (without consent)	
Person: communicate or publish record of conversation or activity	✓ (without consent)	✓ (without consent)	✓ (without consent)	✓ (without consent)	✓ (without consent)
EXCEPTIONS TO THE PROHIBITIONS					
There are other exceptions to these prohibitions that differ between jurisdictions, including for actions to protect a person's lawful interests, in the public interest, for a person's safety and well-being or for a lawful purpose.					
OTHER MATTERS					
Inadmissibility of evidence of a private conversation obtained from use of a listening device	✓ (inadmissible unless exception applies)			✓ (inadmissible if unlawfully obtained, unless exception applies)	
Offence to possess record of unlawfully recorded private conversation or activity	✓ (without consent)	✓ (without consent)			
Offence to manufacture, supply or possess surveillance device for unlawful use	✓	✓	✓ (possess only)		✓ (possess only)
Offence to advertise surveillance device				✓ (listening device)	
Enter dwelling house without consent or by force, threat, deceit, fraud etc				✓	

TAS	VIC	WA	CTH	
				USE PROHIBITION OFFENCES
✓ (without consent)	✓ (without consent where person is not a party; but not an offence where person is a party)	✓ (without consent)		**Listening device:** use, install or maintain a listening device to listen to or record a private conversation
	✓ (without consent where person is not a party; but not an offence where person is a party)	✓ (without consent)		**Optical surveillance device:** use, install or maintain an optical surveillance device to observe or record a private activity
	✓ (without consent)	✓ (without consent)		**Tracking device:** use, install or maintain a tracking device to determine or monitor the geographical location of a person or an object
	✓ (by law enforcement officer; without consent of person on whose behalf information is being input or output)			**Data surveillance device:** use, install or maintain a data surveillance device to monitor or record information input into or output from a computer
			✓ (without the knowledge of the person making the communication)	**Telephone communication:** intercept (including listen to or record) a telephone communication
				COMMUNICATION OR PUBLICATION PROHIBITION OFFENCES
✓ (without consent)				**Party:** communicate or publish record of conversation
✓ (without consent)	✓ (without consent)	✓ (without consent)	✓ (where information obtained by unlawful interception)	**Person:** communicate or publish record of conversation or activity
				EXCEPTIONS TO THE PROHIBITIONS
There are other exceptions to these prohibitions that differ between jurisdictions, including for actions to protect a person's lawful interests, in the public interest, for a person's safety and well-being or for a lawful purpose.				
				OTHER MATTERS
✓ (inadmissible if unlawfully obtained, unless exception applies)				Inadmissibility of evidence of a private conversation obtained from use of a listening device
✓ (without consent)				Offence to possess record of unlawfully recorded private conversation or activity
		✓ (possess only)		Offence to manufacture, supply or possess surveillance device for unlawful use
				Offence to advertise surveillance device
				Enter dwelling house without consent or by force, threat, deceit, fraud etc

Appendix C

Regulation of drones

[C.1] The term 'drone' is commonly used to refer to any remotely controlled or autonomous aircraft or underwater craft.[597] The former is also variously referred to as an aerial drone, remotely piloted aircraft ('RPA'), remotely piloted aircraft system ('RPAS'), unmanned aerial vehicle ('UAV'), unmanned aerial system ('UAS'), unmanned underwater vehicle ('UUV') or autonomous underwater vehicle ('AUV').

[C.2] At an international level, the development of civil aviation standards and recommended practices and policies is the responsibility of the International Civil Aviation Organization ('ICAO'), a specialised agency of the United Nations of which Australia is a member.[598] The ICAO notes that '[t]he rapid rise of [unmanned aircraft systems] raises new challenges that were not considered in historic aviation regulatory frameworks'. In addition to matters of safety, it identifies the rights of property owners, rules of trespass and privacy as key areas of concern. In particular, it notes that:[599]

> Consideration of privacy laws while ensuring a balanced approach to safety and privacy may require responding to complaints about [unmanned aircraft] operating around sensitive areas and critical infrastructure.

[C.3] In Australia, the Civil Aviation Safety Authority ('CASA') is the national authority responsible for regulating aviation safety, including the use of aerial drones.

[C.4] Local governments may also regulate the use of drones on council land, including parks. In the Brisbane City Council region, for example, the launching and landing of drones and other RPAs from council parks is, with some exceptions, a 'restricted activity' under the *Public Land and Council Assets Local Law 2014* and can only be undertaken in designated areas or with council consent.[600]

[C.5] Maritime Safety Queensland has jurisdiction over water space management, including the operation of drones, up to three nautical miles off the Queensland coast. Drone use outside this area, but within Australian waters, is the jurisdiction of the Australian Maritime Safety Authority.[601]

---

597 QDS (2018) 9. The QDS excludes unmanned and remotely or autonomously piloted land vehicles from its scope due to 'the considerable difference in the regulatory and policy environment'.

598 Under the ICAO, *Convention on International Civil Aviation ('Chicago Convention')*, 7 December 1944 (1994) 15 UNTS 295. See generally ICAO, *About ICAO* <https://www.icao.int/about-icao/Pages/default.aspx>.

599 ICAO, *UAS Toolkit: Narrative* [1.1], [1.5], [4.7] <https://www.icao.int/safety/UA/UASToolkit/Pages/Narrative-Background.aspx>.

600 See Brisbane City Council, *Launching drones from Council parks* (5 December 2018) <https://www.brisbane.qld.gov.au/facilities-recreation/parks-venues/parks/using-council-parks/launching-drones-council-parks>; *Public Land and Council Assets Local Law 2014* s 12(1)(e), (2), example. This does not apply to a remotely controlled, powered flying machine or model aircraft which is a children's toy or which weighs less than 0.5 kg: s 12(3)(c). See also ss 9(3)(f), 12(3)(e) as to consent. Several parks across Brisbane have been chosen to include designated areas for launching drones and other RPAs recreationally.

601 QDS Consultation Paper (2017) 5. As yet, there are no regulations specific to the operation of underwater drones.

[C.6] Guidelines, policies and standards have also been, or are being, developed in relation to the use of drones, including by Queensland government agencies.[602]

CASA regulations

[C.7] Part 101 of the *Civil Aviation Safety Regulations 1998* (Cth) sets out requirements for the operation of unmanned aircraft, including RPAs and model aircraft.

[C.8] An aerial drone must not be operated in a way that creates a hazard to another aircraft, another person or property.[603]

[C.9] A person is not required to be licensed or certified by CASA to fly a drone recreationally,[604] or to fly a drone commercially if it weighs between 100 g and 2 kg.[605] However, an aerial drone:[606]

- must only be flown during the day and must be operated within the visual line of sight of the person who is operating it;[607]
- must be operated at or below 400 feet (120 metres) above ground level by day;
- must not be operated within 30 metres of a person who is not directly associated with the operation of the RPA;
- must not be operated—
  - in a prohibited or restricted area;

602 See [C.17], [C.19] below in relation to Queensland government agencies. At an international level, the International Organization for Standardization ('ISO') is currently developing draft international standards for drone operations. It is anticipated that these will be adopted worldwide in 2019, and will address some public concerns surrounding privacy and data protection: See generally ISO, *ISO/TC 20/SC 16: Unmanned aircraft systems* (accessed 13 December 2018) <https://www.iso.org/committee/5336224.html>; sUAS News, *New ISO Draft Standards for Drone Operations released for comment* (21 November 2018) <https://www.suasnews.com/2018/11/new-iso-draft-standards-for-drone-operations-released-for-comment/>.

603 *Civil Aviation Safety Regulations 1998* (Cth) reg 101.055(1).

604 RPAs used for sport or recreational purposes that weigh 150 kg or less are considered to be operating privately and are regulated by the provisions for model aircraft: see CASA, *Flying drones or model aircraft recreationally* (23 June 2018) <https://www.casa.gov.au/modelaircraft>; *Civil Aviation Safety Regulations 1998* (Cth) regs 101.237(3)(a), (5), subpt 101.G.

605 CASA, *Flying drones commercially* (20 February 2018) <https://www.casa.gov.au/standard-page/flying-drones-commercially>; *Civil Aviation Safety Regulations 1998* (Cth) subpt 101.F regs 101.237(3)(b), 101.252(1), 101.270(1). However, the person must register their details with CASA, complete a notification form and fly within standard operating conditions. If the drone weighs more than 2 kg, or the person wants to fly outside the standard procedures, they will need to hold a remote pilot licence and either be certified as an operator, or work for a certified operator: CASA, *Commercial unmanned flight—remotely piloted aircraft under 2 kg* (1 August 2018) <https://www.casa.gov.au/standard-page/commercial-unmanned-flight-remotely-piloted-aircraft-under-2kg>; *Civil Aviation Safety Regulations 1988* (Cth) subpt 101F divs 101F.1, 101F.5.

606 CASA, *Droneflyer: Rules* (2018) <https://droneflyer.gov.au/>; *Civil Aviation Safety Regulations 1998* (Cth) reg 101.238. See also regs 101.385, 101.390, 101.395, 101.400.

607 This means the person operating the RPA must be able to orientate, navigate and see the aircraft with their own eyes at all times (rather than through a device, for example, through binoculars or a telescope): *Civil Aviation Safety Regulations 1998* (Cth) reg 101.073(3).

  - over a populous area;[608] or
  - within three nautical miles (5.5 kilometres) of the movement area of a controlled aerodrome;
  - over an area where a fire, police or other public safety or emergency operation is being conducted without the approval of a person in charge of the operation; and
- must be the only RPA being operated by the person (that is, a person may only operate one RPA at a time).

[C.10] Penalties for breach of operating conditions by drone users include fines of up to 50 penalty units ($10 500).[609]

[C.11] In addition to the standard operating procedures, the *Civil Aviation Safety Regulations 1998* (Cth) provide for a manual of standards for more detailed technical requirements. CASA has recently conducted a public consultation on a draft manual of standards for RPAs covering various matters, including requirements for the operation of RPAs below 400 feet (200 metres) in controlled airspace or near controlled aerodromes and standards for extended visual line of sight operations.[610]

[C.12] CASA recently completed a review of aviation safety regulation of RPA systems. Among other things, CASA expressed support for the mandatory registration in Australia of RPAs weighing more than 250 grams, and education and training for all RPA system operators.[611]

[C.13] CASA does not expressly regulate privacy issues or deal with privacy complaints related to drone use.[612]

---

608 In general terms, a 'populous area' means any area where, if the drone fails, it could cause injury to people or property: *Civil Aviation Safety Regulations 1998* (Cth) reg 101.025.

609 See generally *Civil Aviation Safety Regulations 1998* (Cth) subpts 101.C, 101.F; *Crimes Act 1914* (Cth) s 4AA(1).

610 See *Civil Aviation Safety Regulations 1998* (Cth) reg 101.028; CASA, *Proposed Part 101 (Unmanned aircraft and rockets) Manual of Standards 2018 (CD 1807US)* (2018) <https://consultation.casa.gov.au/regulatory-program/cd1807us/>. The consultation closed in November 2018, with the manual of standards expected to be introduced in 2019.

611 In relation to education and training, CASA considered that it should develop a simple online course for recreational and excluded category RPA operators on safe RPA operations (followed by a quiz with a minimum pass mark) and continue its education and training in respect of remote pilot licenses: CASA, *Review of aviation safety regulation of remotely piloted aircraft systems* (May 2018) 4. See also CASA, *Droneflyer* (2018) <https://droneflyer.gov.au/>.

612 However, the safety pamphlets about the use of RPAs, available at CASA, *Drone resources and links* (12 September 2018) <https://www.casa.gov.au/operations/standard-page/rpa-resources-and-links>, include the following statement:

> **Respect personal privacy**. Don't record or photograph people without their consent—this may breach state laws.

This gives effect to the Eyes in the Sky Report (2014) Rec 2.

Privacy

Invasion of Privacy Act 1971

[C.14] Because the *Invasion of Privacy Act 1971* regulates listening devices but not optical surveillance devices or other surveillance devices, it does not apply to video footage or images (without sound) captured by drones.

Queensland Drones Strategy

[C.15] Drones are increasingly accessible, with less expensive platforms becoming available that support advanced capabilities for recording images, videos and audio. The Queensland Drones Strategy (the 'QDS') noted that this raises a number of challenges and concerns in relation to privacy.[613] One of the actions arising out of the QDS was to:[614]

> Refer the question of whether Queensland's legislation adequately protects individuals' privacy in the context of modern and emerging technologies to the Queensland Law Reform Commission.

[C.16] Another action is for the development and implementation of an education campaign, targeted at recreational drone users, 'to provide information on the safe and proper use of drones and respecting others' privacy'.[615]

[C.17] The QDS includes a number of actions relating to the development of relevant guidelines and policies, including the development of an internal Queensland Government Drones Use Policy to provide information to Queensland government agencies regarding the use of drones. This is being led by the Department of Transport and Main Roads.[616]

[C.18] The QDS has also led to the establishment of a working group 'to help achieve consistency in the use of drones across local government areas, including recreational and commercial use'.[617]

Office of the Information Commissioner (Qld)

[C.19] The Office of the Information Commissioner (Qld) has released a guideline on drones and the privacy principles.[618] The guideline applies to Queensland government agencies and relates to information privacy.

[C.20] Queensland government agencies that capture personal information using a drone must ensure that the collection, storage, use and disclosure of that

---

613 QDS (2018) 31.

614 Ibid 33.

615 Ibid.

616 Ibid 37.

617 Ibid 33. The working group is led by the Department of Local Government, Racing and Multicultural Affairs, with the Local Government Association of Queensland, individual local governments and relevant government agencies.

618 Office of the Information Commissioner (Qld), *Guideline: Drones and the Privacy Principles* (16 April 2018). See also [2.110]–[2.111] above.

information complies with the privacy obligations in the *Information Privacy Act 2009*. 'Personal information' is any information about an individual who is or can reasonably be identified.[619] This would include, for example, a video or audio recording of an individual's image or voice captured by drone, where the quality of the recording is such that the individual can be reasonably identified.

[C.21] The *Information Privacy Act 2009* applies only to Queensland government agencies. Accordingly, the Privacy Commissioner established under that Act, within the Office of the Information Commissioner (Qld), has no role to regulate, or determine privacy complaints in respect of, the use of drones by individuals or businesses.[620]

Commonwealth

[C.22] The *Privacy Act 1988* (Cth) applies only to certain entities. It does not regulate or cover privacy complaints in respect of the use of drones by individuals or by small businesses.[621]

[C.23] The Australian Parliament's House of Representatives Standing Committee on Social Policy and Legal Affairs tabled the Eyes in the Sky Report in July 2014. Among other things, the report recommended that the Australian government:[622]

- consider introducing legislation to provide protection against privacy invasive technologies, including RPAs, with particular emphasis on protecting against intrusions on a person's seclusion or private affairs;
- initiate action to simplify Australia's privacy regime by introducing harmonised national surveillance laws that cover the use of listening devices, optical surveillance devices, data surveillance devices and tracking devices; and
- coordinate with CASA and the Australian Privacy Commissioner to review the adequacy of the privacy and air safety regimes in relation to drones.

[C.24] The Commonwealth government tabled its response in December 2016.[623] It did not support the first of those recommendations. Specifically, it did not support the establishment of a separate tort on privacy.[624] It noted the recommendation for the harmonisation of surveillance devices legislation, but considered it is 'appropriate

---

619 *Information Privacy Act 2009* (Qld) s 12. See the discussion at [2.104] ff above.

620 See the discussion at [2.104] ff above.

621 See the discussion at [2.112] ff above. With respect to businesses, the *Privacy Act 1988* (Cth) applies to businesses which trade in personal information and private sector organisations with an annual turnover of more than $3 million.

622 Eyes in the Sky Report (2014) Recs 3, 4, 6.

623 Eyes in the Sky Report: Government Response (2016).

624 Ibid 8, stating:

> Introducing a new cause of action would only add to the regulatory burden on business, which is contrary to the government's commitment to reducing red tape. The common law already provides avenues for individuals to seek redress for the torts of trespass, nuisance, defamation and breach of confidence. The states and territories also have their own legislation.

that states and territories continue to modify their own surveillance device laws, if necessary'.[625] It also noted the last recommendation, responding that:[626]

> Issues of air safety and privacy are however regulated by separate means, through separate legislation and by separate Government agencies.
>
> It is appropriate then that reviews of the adequacy of the air safety and the privacy regimes are conducted by the agency with expertise and responsibility for each area: CASA for air safety and the Attorney-General's Department, in consultation with the Office of the Australian Information Commissioner, for privacy matters.
>
> …
>
> The Attorney-General's Department will continue to liaise with CASA as required, in consultation with the Office of the Australian Information Commissioner, on issues regarding privacy and air safety in relation to RPAS, with a view to addressing particular regulatory issues and any emerging areas of action.

[C.25] In July 2018, the Australian Parliament's Senate Rural and Regional Affairs and Transport References Committee released its report on the inquiry into regulatory requirements that impact on the safe use of RPAS, UAS and associated systems. The focus of the inquiry was safety and regulation, and not the regulation of the privacy implications of drones. The Committee recommended that, '[a]s part of a whole of government policy approach, … harmonisation of state and territory privacy laws should also be considered'. The committee otherwise left issues of privacy 'to the ongoing consideration of government'.[627]

625 Ibid 9.

626 Ibid 10.

627 Senate Rural and Regional Affairs and Transport References Committee, Parliament of Australia, C*urrent and future regulatory requirements that impact on the safe commercial and recreational use of Remotely Piloted Aircraft Systems (RPAS), Unmanned Aerial Systems (UAS) and associated systems* (July 2018) [1.12], [8.45], Rec 8.

Appendix D

Civil surveillance law reform reviews in other jurisdictions

[D.1] Recent law reform reviews and other inquiries which have considered surveillance regulation in Australia include:

- New South Wales Law Reform Commission ('NSWLRC'), *Surveillance: an interim report*, Report No 98 (February 2001) and *Surveillance*, Report No 108 (May 2005);
- Victorian Law Reform Commission ('VLRC'), *Surveillance in Public Places*, Consultation Paper No 7 (March 2009) and *Surveillance in Public Places*, Report No 18 (June 2010);
- Australian Law Reform Commission ('ALRC'), *Serious Invasions of Privacy in the Digital Era*, Discussion Paper No 80 (March 2014) and *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014); and
- D Stewart, 'Review of ACT Civil Surveillance Regulation' (Report, June 2016).

New South Wales Law Reform Commission

[D.2] The NSWLRC received a reference in 1996, which required it to inquire into and report on the scope and operation of the *Listening Devices Act 1984* (NSW), the need to regulate the use of visual surveillance equipment and other related matters. The NSWLRC provided an interim report in 2001, supplemented by a final report in 2005.[628]

[D.3] The NSWLRC concluded that the regulation of surveillance should not be device specific to ensure that the law is not outpaced by technological developments. Regulation should be sufficiently broad to capture all devices that might be used to conduct surveillance, including those that may be developed in the future.[629]

[D.4] The NSWLRC did not adopt a distinction between public and private places or activities as a basis for regulation. It considered that the term 'public place' lacks clarity and that distinctions between 'public' and 'private' spaces are diminishing with technological advances. It also considered that the legislative concepts of 'private conversation' and 'private activity' contained aspects that were difficult to establish

---

628 NSWLRC Interim Report No 98 (2001); NSWLRC Report No 108 (2005). The interim report developed a proposed legislative framework for the regulation of surveillance. In its final report, the NSWLRC stated that this proposed framework remained 'sound' and explained that the final report canvassed only those issues that required amendment or clarification as a result of subsequent legal or other developments. Consequently, the NSWLRC stated that the interim and final reports should be read in conjunction: NSWLRC Report No 108 (2005) [1.19]–[1.23].

629 NSWLRC Interim Report No 98 (2001) [2.15]–[2.19], [2.33]–[2.39], Recs 1 to 3. See the discussion at [3.33] ff above.

and did not encompass all potentially invasive surveillance activity, and therefore that they did not sufficiently protect privacy.[630]

[D.5] Instead, the NSWLRC considered that the regulation of surveillance should distinguish between surveillance that occurs with ('overtly') or without ('covertly') the knowledge of the subject. Under the proposed scheme, a person would be assumed to have knowledge of surveillance if given adequate prior notice, for example, in the form of clearly visible signs or surveillance equipment (even if not actually read or observed by the person).[631]

[D.6] The NSWLRC proposed that overt surveillance should be regulated by a set of legislative principles, for example, that surveillance must be used only for lawful purposes and that its use must not exceed the intended purpose. It was also proposed that 'larger' users, such as banks, be required to supplement those principles with tailored codes of practice.[632]

[D.7] The NSWLRC proposed that covert surveillance should require prior authorisation or, where that is not possible or practicable, retrospective validation. The proposed scheme developed three different, but complementary, approaches for surveillance depending on whether it is conducted by law enforcement agencies, in the public interest or in an employment context.[633] The NSWLRC also concluded that the regulatory scheme for covert surveillance should not permit a party to record a private conversation or activity without the knowledge of the other participants ('participant monitoring').[634]

[D.8] The NSWLRC concluded that legislation should apply to all persons or agencies conducting surveillance, and should not have the effect of regulating only particular categories of people.[635]

[D.9] It also considered that the scheme should distinguish between surveillance and data protection. It recommended that the 'random or overt collection, retrieval and matching of information on computer databases' should not be included in the scheme.[636]

[D.10] The regulatory scheme proposed by the NSWLRC has not been implemented. Subsequent to the final report, new legislation was introduced in New South Wales which did not follow the suggested approach of the NSWLRC. That legislation generally maintained the traditional regulatory approach, but modernised and clarified the law.[637]

---

630 Ibid [2.20]–[2.27].

631 Ibid [2.77]–[2.79], [2.88], Recs 9, 10, 13.

632 Ibid [2.86]–[2.87]; see generally chs 3, 4.

633 Ibid [2.32], [2.89]–[2.98]; see respectively chs 5, 6, 7.

634 Ibid [2.99]–[2.107], Rec 14; see also app A. See the discussion at [3.82] ff above.

635 Ibid [2.28]–[2.32].

636 Ibid [2.68]–[2.73], Recs 6, 7.

637 See the *Surveillance Devices Act 2007* (NSW) which replaced the *Listening Devices Act 1984* (NSW).

Victorian Law Reform Commission

[D.11] In 2010, the VLRC completed a review on surveillance in public places.[638] This was the second part of a two stage reference about privacy.[639]

[D.12] This review was limited to a consideration of whether there is appropriate control of surveillance in public places.[640] The VLRC considered that public place surveillance has both risks and benefits, and that 'any regulation of public place surveillance must be flexible enough to balance the many competing interests'.[641]

[D.13] The VLRC therefore recommended principles-based regulation to promote the responsible use of surveillance in public places.[642] In particular, it recommended that legislation should include the following six overarching principles to guide all users about responsible use of public place surveillance:[643]

1. People are entitled to a reasonable expectation of privacy when in public places.

2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals.

3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices.

4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.

5. Public place surveillance should be proportion[ate] to its legitimate purpose.

6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

[D.14] The VLRC recommended that there should be an independent regulator responsible for the oversight of public place surveillance in Victoria. The primary function of the regulator would be to promote responsible use of public place

638 The terms of reference, received in 2002, asked the VLRC to inquire into and report on 'whether legislative or other measures are necessary to ensure that there is appropriate control of surveillance, including current and emerging methods of surveillance'. The VLRC published a consultation paper in 2009 and a final report in 2010: VLRC Consultation Paper No 7 (2009); VLRC Report No 18 (2010).

639 The first part of the reference covered workplace privacy, resulting in a report tabled in 2005: VLRC, *Workplace Privacy* (12 November 2018) <https://www.lawreform.vic.gov.au/all-projects/workplace-privacy>.

640 The VLRC noted that it is often difficult to delineate between a 'public place' and a 'private place'. It suggested that 'public place' should be understood 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'. A 'public place' would include public areas such as parks and streets, as well as government or privately owned places when they are open to the general public, such as shopping centres, sporting arenas and local swimming pools: see VLRC Report No 18 (2010) [1.1]–[1.2], [1.15]–[1.17]. See also VLRC Consultation Paper No 7 (2009) [1.19]-[1.21].

641 VLRC Report No 18 (2010) [4.138]–[4.141].

642 Ibid [5.1]. The VLRC stated that 'this approach is primarily educative and focuses on achieving best practice use of surveillance technology, while also ensuring that the privacy rights of individuals are adequately protected': 12.

643 Ibid [5.1], [5.4] ff, Rec 2.

surveillance, including by developing best practice guidelines and providing advice to ensure compliance.[644]

[D.15] At the same time, the VLRC recognised that 'guidance alone cannot protect people from some practices that seriously affect their privacy'.[645] It therefore recommended a number of regulatory measures to modernise and strengthen the *Surveillance Devices Act 1999* (Vic) ('the Act'). In particular, it recommended that:

- the Act 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 the use of surveillance devices;[646]
- the Act 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;[647]
- the Act should prohibit participant monitoring except in limited circumstances, including with the consent of a principal party to the private conversation or activity where the recording is reasonably necessary to protect that party's lawful interests;[648]
- the definition of 'private activity' should be amended so that it includes a private activity whether it is carried on inside or outside a building;[649]
- the definition of 'tracking device' should be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object;[650] and

644 Ibid 13, Recs 3 to 9. The VLRC recommended that the functions of the regulator should be exercised by the Victorian Privacy Commissioner.

645 Ibid [5.3], 13.

646 Ibid [6.15] ff, Rec 12. The VLRC observed that the notion of consent—particularly implied consent—is sometimes difficult to characterise when dealing with many common surveillance practices in public places. To address this, it considered that the *Surveillance Devices Act 1999* (Vic) should actively encourage the practice of giving adequate notice of surveillance, by signage or other means.

647 Ibid [6.24]–[6.28], Rec 13. The VLRC noted that this is in keeping with public expectations.

648 Ibid [6.54]–[6.58], [6.59] ff, Rec 18. The VLRC considered that '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'. For example, it noted that the *Surveillance Devices Act 1999* (Vic) currently permits a participant in sexual activity to record that activity without the knowledge or consent of the other party involved (although the publication of information obtained through participant monitoring is prohibited): [6.56]–[6.57].

649 Ibid [6.7] ff, Rec 11. Currently, an activity cannot be a 'private activity' under the *Surveillance Devices Act 1999* (Vic) if it occurs outside a building. Consequently, there is no protection in relation to private activities in outdoor places, such as backyards. In contrast, a conversation may be a 'private conversation' regardless of where it occurs.

650 Ibid [6.29] ff, Rec 14. Currently, the definition of 'tracking device' in s 3(1) of the *Surveillance Devices Act 1999* (Vic) is limited to 'an electronic device the primary purpose of which is to determine the geographical location of a person or an object'. Consequently, a device that is capable of tracking, but is not primarily used for that purpose (such as a mobile phone with GPS capability), is not a tracking device within the meaning of the Act.

- more serious types of behaviour, such as the use of a surveillance device to intimidate, demean or harass another person, should be covered by a criminal offence.[651]

[D.16] The VLRC recommended that a civil penalty regime should also apply to the criminal offences in the Act.[652] The regulator would be able to seek civil penalties for breaches of the principal offences in the Act, when this course is preferable to criminal prosecutions.[653]

[D.17] The VLRC's recommendations have not been implemented. However, since the report was tabled, a number of guidelines have been released on the use of surveillance and CCTV that refer to the guiding principles for surveillance in public places recommended in the VLRC's report.[654]

Australian Law Reform Commission

[D.18] In 2013, the ALRC received terms of reference to inquire into the prevention of and remedies for serious invasions of privacy in the digital era. Among other things, the reference was made having regard to 'the rapid growth in capabilities and use of information, surveillance and communication technologies'.[655]

[D.19] The ALRC report, released in 2014, considered a range of matters relating to the protection of privacy,[656] including surveillance devices legislation.[657]

[D.20] Relevantly, the ALRC made seven recommendations about surveillance devices legislation, namely, for:[658]

- the replacement of existing state and territory legislation with Commonwealth legislation, to ensure national consistency;
- 'technology neutral' legislation that would regulate the devices recognised under existing laws (namely, listening devices, optical surveillance devices, tracking devices and data surveillance devices) as well as applying to new

---

651 Ibid [6.94] ff, Recs 20, 21. See the discussion at [3.253] ff above.

652 Ibid [6.82] ff, Recs 19, 21.

653 Ibid [5.44]. See discussions at [3.229], [3.316]–[3.317] above.

654 See Victorian Ombudsman, *Closed Circuit Television in Public Places—Guidelines: Victorian Ombudsman's Guidelines for Developing Closed Circuit Television Policies for Victorian Public Sector Bodies* (November 2012); Office of the Victorian Information Commissioner (formerly Commissioner for Privacy and Data Protection), *Guidelines to Surveillance and Privacy in the Victorian Public Sector* (May 2017); Victoria State Government, *Guide to Developing CCTV for Public Safety in Victoria: A Community Crime Prevention Initiative* (June 2018). See generally VLRC, *Surveillance in Public Places* (12 November 2018) <https://www.lawreform.vic.gov.au/all-projects/surveillance-public-places>.

655 See ALRC, *Terms of Reference: Serious invasions of privacy in the digital era* (27 March 2014) <https://www.alrc.gov.au/inquiries/invasions-privacy/terms-reference>. This followed earlier reviews on privacy matters, including ALRC Report No 22 (1983), which led to the enactment of the *Privacy Act 1988* (Cth), and ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (May 2008), which reviewed that Act.

656 The terms of reference required the ALRC to design a statutory cause of action for serious invasions of privacy and to consider other innovative ways in which law may reduce serious invasions of privacy in the digital era: ibid.

657 See ALRC Report No 123 (2014) ch 14.

658 Ibid Recs 14-1 to 14-8. Rec 14-6 related to workplace surveillance laws and is not considered here.

devices (such as drones) and technologies which are not 'devices' in the traditional sense (such as software or networked systems);[659]

- the integration of the proposed new Commonwealth surveillance legislation with existing Commonwealth telecommunications interception legislation;
- the removal of provisions that permit participant monitoring;
- the inclusion of a 'responsible journalism' defence to permit journalists and media groups to use surveillance devices in limited circumstances relating to matters of public concern and importance;
- provisions empowering a court to order remedial relief, including compensation, where an individual is subjected to unlawful surveillance;[660] and
- conferral of jurisdiction on state and territory courts or tribunals to hear disputes between residential neighbours about the use of surveillance devices.[661]

[D.21] The ALRC concluded that 'the existing, technology specific laws lead to inadequate protections from surveillance'.[662] Overall, the ALRC observed that:[663]

> Surveillance device laws provide important privacy protection. The legislation offers some protection against intrusion into seclusion and against the collection of some information, such as recordings of private conversations. Consistency in these laws is important both for protecting individuals' privacy and for reducing the compliance burden on organisations that use surveillance devices in multiple jurisdictions.

[D.22] The ALRC's recommendation for Commonwealth surveillance legislation has not been implemented; this remains the subject of state and territory laws. In most jurisdictions, the surveillance devices legislation regulates both civil surveillance as well as surveillance by law enforcement agencies, with the latter reflecting national model provisions to facilitate cross-border investigations.[664]

---

659 See the discussion at [3.39] ff above.

660 See the discussion at [3.278] ff above.

661 See the discussion at [3.305] ff above.

662 ALRC Report No 123 (2014) [14.33].

663 Ibid [14.9]. See also [14.1]–[14.2].

664 In Queensland, unlike the other states and territories, the law enforcement provisions are included in separate legislation: see [2.82] ff above.

Australian Capital Territory review

[D.23] In 2016, the ACT government commissioned an independent review of the regulation of non-government surveillance in the Australian Capital Territory, including consideration of gaps and areas for reform (the 'ACT review').[665]

[D.24] In the Australian Capital Territory, the *Listening Devices Act 1992* (ACT) applies to listening devices, but not to optical surveillance, data surveillance or tracking devices. In the ACT Review, it was recommended, among other things, that the *Listening Devices Act 1992* (ACT) should:[666]

- be renamed the 'Surveillance Act' and amended to include 'restrictions on other forms of surveillance activity', such as visual observation, data collection and tracking;
- make clear that the concepts of 'private conversation' and 'private activity' are limited where the parties to a conversation or activity could reasonably expect to be overheard or observed by others;
- not permit participant monitoring;
- for any exception involving a person's 'lawful interests', require an objective evaluation of the purpose of the surveillance or communication and whether it is necessary and proportionate;
- permit surveillance that is carried out to protect a 'public interest', where the surveillance activity is necessary and proportionate (but, require a court order for communication of such information unless the communication is made to a media organisation that is subject to an appropriate code of conduct);
- where consent is an element, require that the consenting person is adequately informed, has the capacity to understand and communicate their consent, and provides consent that is voluntary, current and specific;
- not extend to inadvertent observation of a private activity, including by a drone or other UAV (but appropriately regulate the communication of information that is inadvertently obtained);
- provide that prohibitions on tracking the geographical location of a person or object include tracking through the use of a network or computer system, including access to metadata or other information;
- not include any specific exemptions for private investigators or others who conduct surveillance for remuneration, because they are not presently subject to an effective licensing system; and

665 ACT Review (2016) [1.1]. The review was announced by the Minister for Justice and Consumer Affairs and the reviewer engaged by the Justice and Community Safety Directorate: see Minister for Justice and Consumer Affairs, 'Review of civil surveillance to modernise ACT privacy laws' (Ministerial Media Statement, 5 May 2016); Justice and Community Safety Directorate (ACT), *Review of Civil Surveillance in the ACT* (2016) <http://www.justice.act.gov.au/review/view/45/title/review-of-civil-surveillance-in>.

666 ACT Review (2016) [2.5](a)–(i), [6.9]–[6.11]; see also pt 6.

- preserve the court's discretion to admit evidence obtained through the use of a surveillance device in certain circumstances.

[D.25] In the ACT Review, it was also recommended that consideration be given to providing 'remedial options' for individuals subject to unlawful surveillance, such as access to the ACT Civil and Administrative Tribunal to seek monetary compensation.[667]

[D.26] The ACT government called for submissions on the review 'to inform a response to the recommendations, and consideration of reforms to surveillance legislation to encourage the responsible use of new and emerging technologies' and to protect personal privacy.[668] The recommendations have not been implemented.

667 Ibid [2.5](j), [6.46]–[6.47].

668 Justice and Community Safety Directorate (ACT), *Review of Civil Surveillance in the ACT* (2016) <http://www.justice.act.gov.au/review/view/45/title/review-of-civil-surveillance-in>

Appendix E

International human rights and privacy instruments

Privacy

[E.1] A right to privacy is recognised in international human rights instruments to which Australia is a signatory, including the *Universal Declaration of Human Rights* ('UDHR') and the *International Covenant on Civil and Political Rights* ('ICCPR').[669]

[E.2] Article 17 of the ICCPR provides that:[670]

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> Everyone has the right to the protection of the law against such interference or attacks.

[E.3] The United Nations Human Rights Committee explains that the obligations imposed by article 17 require state parties to 'adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right'. Relevantly, the Committee observes that:[671]

> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire tapping and recording of conversations should be prohibited. Searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment.
>
> …
>
> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the [ICCPR]. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

---

669 *Universal Declaration of Human Rights*, GA Res 217A (III), 10 December 1948 ('UDHR') art 12; *International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), 16 December 1966 ('ICCPR') art 17.

670 UDHR art 12 is in similar terms.

671 Human Rights Committee, *General Comment No 16: Article 17 (Right to privacy)*, 32nd sess (8 April 1988) [1], [8]–[10].

[E.4] A right to privacy, in similar terms to article 17 of the ICCPR, is also recognised in other international human rights instruments and in the human rights statues of some other jurisdictions.[672]

[E.5] In Australia, the *Human Rights Act 2004* (ACT) and the *Charter of Human Rights and Responsibilities Act 2006* (Vic) provide, in virtually the same terms, that a person 'has the right' not to have their 'privacy, family, home or correspondence' unlawfully or arbitrarily interfered with and not to have their 'reputation unlawfully attacked'.[673] In Queensland, the Human Rights Bill 2018 also includes this right:[674]

> **25 Privacy and reputation**
>
> A person has the right—
>
> (a) not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
>
> (b) not to have the person's reputation unlawfully attacked.

Information privacy

[E.6] The protection of information privacy is recognised at the international level by the OECD's *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* ('OECD Guidelines').[675]

[E.7] The OECD Guidelines recognise member countries' common interest in 'promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information'.[676] They provide seven principles for public and private sector dealings with personal data, covering the collection, accuracy, purpose, use and security of personal data, as well as access to and information about data and data policies. Relevantly, the 'collection limitation principle' provides that:[677]

> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

---

672 See, eg, *Convention for the Protection of Human Rights and Fundamental Freedoms*, 213 UNTS 221/ETS No 5, as amended by Protocols No 11 and 14 (the 'European Convention on Human Rights') art 8; American Convention on Human Rights, OAS Treaty Series No 36 (1960) art 11; *Charter of Fundamental Rights of the European Union*, arts 7 and 8.

673 *Human Rights Act 2004* (ACT) s 12; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.

674 Human Rights Bill 2018 (Qld) cl 25. This is intended to establish statutory protection for the rights recognised in the ICCPR art 17: Explanatory Notes, Human Rights Bill 2018 (Qld) 2, 3–4.

675 OECD, 'Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' in *The OECD Privacy Framework* (2013) pt 1 ch 1. Australia is one of several member countries of the Organisation for Economic Co-operation and Development ('OECD').

676 Ibid preamble.

677 Ibid cl 7.

[E.8] The OECD Guidelines, first adopted in 1980, were revised in 2013 to take account of significant changes in the role of personal information, including:[678]

- The ***volume*** of personal data being collected, used and stored;
- The ***range of analytics*** involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- The ***value*** of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- The extent of ***threats*** to privacy;
- The ***number and variety of actors*** capable of either putting privacy at risk or protecting privacy;
- The ***frequency and complexity of interactions*** involving personal data that individuals are expected to understand and negotiate;
- The ***global availability*** of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows. (emphasis in original)

[E.9] The OECD Guidelines informed the privacy principles adopted under the *Privacy Act 1998* (Cth).[679]

Freedom of expression and opinion

[E.10] The protection of privacy must be balanced against other legitimate public interests. In the context of article 17 of the ICCPR, interference with the right to privacy must be for a 'legitimate aim' and to an extent that is reasonable, that is, 'necessary' and 'proportionate' to the end sought.[680]

[E.11] Freedom of expression and opinion, like privacy, is recognised as a fundamental human right in the UDHR and the ICCPR.[681] Article 19(2) of the ICCPR provides that:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

[E.12] Interference with the right to freedom of expression under article 19 of the ICCPR must be 'necessary' for the protection of others' rights or the protection of national security, public order, public health or morals, and must be 'proportionate'.[682]

---

678 OECD, *The OECD Privacy Framework* (2013) 3–4.

679 Australia, *Parliamentary Debates*, House of Representatives, 1 November 1998, 2117 (L Bowen, Attorney-General).

680 Human Rights Committee, *Views: Communication No 488/1992*, 50th sess, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) ('*Toonen v Australia*').

681 UDHR art 19; ICCPR art 19. The ICCPR art 19(2) is in similar terms to the UDHR art 19.

682 ICCPR art 19(3); Human Rights Committee, *General Comment No 34: Article 19*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [22].

[E.13] Freedom of expression is also recognised in other international human rights instruments and in the human rights statutes of some other jurisdictions.[683]

[E.14] In Australia, the *Human Rights Act 2004* (ACT) and the *Charter of Human Rights and Responsibilities Act 2006* (Vic) provide, in similar terms, that a person 'has the right to freedom of expression', including 'the freedom to seek, receive and impart information and ideas of all kinds', regardless of borders, whether orally, in writing or in print, by way of art, or in another way they choose.[684] In Queensland, the Human Rights Bill 2018 also includes this right:[685]

> **21 Freedom of expression**
>
> (1) Every person has the right to hold an opinion without interference.
>
> (2) Every person has the right to freedom of expression which includes the freedom to seek, receive and impart information and ideas of all kinds, whether within or outside Queensland and whether—
>
> (a) orally; or
>
> (b) in writing; or
>
> (c) in print; or
>
> (d) by way of art; or
>
> (e) in another medium chosen by the person.

[E.15] The Australian Constitution does not expressly protect a right to freedom of expression, but an implied freedom of political communication is recognised as a necessary part of the system of representative and responsible government established by the Constitution.[686]

---

683 See, eg, European Convention on Human Rights, art 10; American Convention on Human Rights, OAS Treaty Series No 36 (1960) art 13; *Charter of Fundamental Rights of the European Union*, art 11.

684 *Human Rights Act 2004* (ACT) s 16; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 15.

685 Human Rights Bill 2018 (Qld) cl 21. This is intended to establish statutory protection for the rights recognised in the ICCPR art 19: Explanatory Notes, Human Rights Bill 2018 (Qld) 2, 3.

686 *Brown v Tasmania* (2017) 349 ALR 398.