



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

Report



**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**

**Report**

Report No 77  
February 2020

Postal address: PO Box 13312, George Street Post Shop, Qld 4003  
Telephone: (07) 3564 7777  
Facsimile: (07) 3564 7794  
Email: [lawreform.commission@justice.qld.gov.au](mailto:lawreform.commission@justice.qld.gov.au)  
Website: [www.qlrc.qld.gov.au](http://www.qlrc.qld.gov.au)

© State of Queensland (Queensland Law Reform Commission) 2020

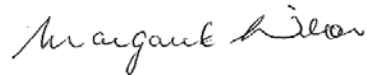
ISBN: 978-0-6481164-4-8

To: The Honourable Yvette D'Ath MP  
Attorney-General and Minister for Justice  
Leader of the House

In accordance with section 15 of the *Law Reform Commission Act 1968*, the Commission is pleased to present its Report, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies*.



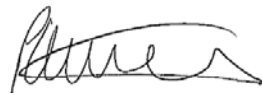
The Honourable Justice David Jackson  
Chairperson



The Honourable Margaret Wilson QC  
Member



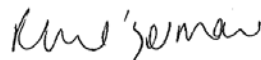
His Honourable Judge Brian Devereaux SC  
Member



Ms Penelope White  
Member



Dr Nigel Stobbs  
Member



Ms Ruth O'Gorman  
Member



### **COMMISSION MEMBERS**

Chairperson:	<b>The Hon Justice David Jackson</b>
Part-time members:	<b>The Hon Margaret Wilson QC His Hon Judge Brian Devereaux SC Ms Penelope White Dr Nigel Stobbs Ms Ruth O’Gorman</b>

### **SECRETARIAT**

Director:	<b>Mr David Groth</b>
Assistant Director:	<b>Mrs Cathy Green</b>
Secretary:	<b>Mrs Jenny Manthey</b>
Senior Legal Officers:	<b>Ms Anita Galeazzi Mrs Elise Ho Ms Paula Rogers</b>
Administrative Officers:	<b>Ms Kahren Giles Mrs Brie Henri</b>

Previous Queensland Law Reform Commission publication in this reference:

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 (2018)

# Abbreviations and Glossary

<b>AAUS</b>	Australian Association for Unmanned Systems
<b>AAUS and Liberty Victoria Paper (2015)</b>	Australian Association for Unmanned Systems and Liberty Victoria, 'The Use of Drones in Australia: An Agenda for Reform' (May 2015)
<b>ACCC</b>	Australian Competition and Consumer Commission
<b>ACCC Digital Platforms Inquiry Report (2019)</b>	Australian Competition and Consumer Commission, <i>Digital Platforms Inquiry</i> , Final Report (June 2019)
<b>ACT Review (2016)</b>	D Stewart, 'Review of ACT Civil Surveillance Regulation' (Report, June 2016)
<b>AHRC</b>	Australian Human Rights Commission
<b>AHRC Discussion Paper (2019)</b>	Australian Human Rights Commission, <i>Human Rights and Technology</i> , Discussion Paper (December 2019)
<b>ALRC</b>	Australian Law Reform Commission
<b>ALRC Discussion Paper No 80 (2014)</b>	Australian Law Reform Commission, <i>Serious Invasions of Privacy in the Digital Era</i> , Discussion Paper No 80 (March 2014)
<b>ALRC Report No 123 (2014)</b>	Australian Law Reform Commission, <i>Serious Invasions of Privacy in the Digital Era</i> , Report No 123 (June 2014)
<b>ALRC Report No 108 (2008)</b>	Australian Law Reform Commission, <i>For Your Information: Australian Privacy Law and Practice</i> , Report No 108 (May 2008)
<b>ALRC Report No 22 (1983)</b>	Australian Law Reform Commission, <i>Privacy</i> , Report No 22 (1983)
<b>APP entity</b>	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 that trades in personal information. An APP entity is required to comply with the <i>Privacy Act 1988</i> (Cth).
<b>APPs</b>	Australian Privacy Principles, under the <i>Privacy Act 1988</i> (Cth)
<b>Australian Government Issues Paper: Serious Invasion of Privacy (2011)</b>	Australian Government, 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, September 2011)
<b>Big data</b>	An extremely large data set that can be mined for patterns, trends and associations, as in relation to human behaviour.
<b>CASA</b>	Civil Aviation Safety Authority
<b>CCTV</b>	closed circuit television
<b>communication or publication prohibitions</b>	The prohibitions under surveillance devices legislation against the communication or publication of information obtained from the use of a surveillance device.



<b>covert surveillance</b>	Surveillance that is done in such a way that the subject of surveillance is unaware that the surveillance is occurring, for example, where the surveillance device is concealed.
<b>the draft Bill</b>	Surveillance Devices Bill 2020, contained in Appendix F
<b>DSDMIP</b>	Department of State Development, Manufacturing, Infrastructure and Planning
<b>drone</b>	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. They are also referred to variously as an autonomous underwater vehicle ('AUV'), remotely piloted aircraft ('RPA'), remotely piloted aircraft system ('RPAS'), unmanned aerial vehicle ('UAV'), unmanned aerial system ('UAS') or unmanned underwater vehicle ('UUV').
<b>Eyes in the Sky Report (2014)</b>	House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, <i>Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy</i> (July 2014)
<b>Eyes in the Sky Report: Government Response (2016)</b>	Australian Government, 'Australian Government Response to the Standing Committee on Social Policy and Legal Affairs Report: <i>Eyes in the Sky: Inquiry into drones and the regulation of air safety and privacy</i> ' (December 2016)
<b>GPS</b>	global positioning system
<b>ICT</b>	information communication technology
<b>IP Act</b>	<i>Information Privacy Act 2009</i> (Qld)
<b>IPPs</b>	Information Privacy Principles, under the <i>Information Privacy Act 2009</i> (Qld)
<b>Joint Working Group Report (2003)</b>	Standing Committee of Attorneys-General and the Australasian Police Ministers Council Joint Working Group on National Investigation Powers, <i>Cross-Border Investigative Powers for Law Enforcement</i> , Report (November 2003)
<b>LRC Ireland</b>	Law Reform Commission of Ireland
<b>LRC Ireland Report No 57 (1998)</b>	Law Reform Commission of Ireland, <i>Privacy: Surveillance and the Interception of Communications</i> , Report No 57 (June 1998)
<b>NSW Parliamentary Committee Report (2016)</b>	Standing Committee on Law and Justice, Parliament of New South Wales, <i>Remedies for the serious invasion of privacy in New South Wales</i> (3 March 2016)
<b>NSWLRC</b>	New South Wales Law Reform Commission
<b>NSWLRC Interim Report No 98 (2001)</b>	New South Wales Law Reform Commission, <i>Surveillance: an interim report</i> , Report No 98 (February 2001)
<b>NSWLRC Issues Paper No 12 (1997)</b>	New South Wales Law Reform Commission, <i>Surveillance</i> , Issues Paper No 12 (May 1997)

<b>NSWLRC Report No 108 (2005)</b>	New South Wales Law Reform Commission, <i>Surveillance</i> , Report No 108 (May 2005)
<b>NSWLRC Report No 120 (2009)</b>	New South Wales Law Reform Commission, <i>Invasion of Privacy</i> , Report No 120 (April 2009)
<b>NZLC</b>	New Zealand Law Commission
<b>NZLC Issues Paper No 14 (2009)</b>	New Zealand Law Commission, <i>Invasion of Privacy: Penalties and Remedies—Review of the Law of Privacy Stage 3</i> , Issues Paper No 14 (March 2009)
<b>NZLC Report No 113 (2010)</b>	New Zealand Law Commission, <i>Invasion of Privacy: Penalties and Remedies—Review of the Law of Privacy Stage 3</i> , Report No 113 (January 2010)
<b>NZLC Study Paper No 19 (2008)</b>	New Zealand Law Commission, <i>Privacy: Concepts and Issues—Review of the Law of Privacy Stage 1</i> , Study Paper No 19 (January 2008)
<b>OAIC</b>	Office of the Australian Information Commissioner
<b>OAIC Guideline: Key concepts—Consent (2019)</b>	Office of the Australian Information Commissioner, 'Chapter B: Key concepts—Consent' in <i>Australian Privacy Principles guidelines</i> (v 1.3, 22 July 2019) < <a href="https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/">https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/</a> >
<b>OAIC, Disclosing information about patients with impaired capacity (2019)</b>	Office of the Australian Information Commissioner, 'Chapter 7: Disclosing information about patients with impaired capacity' in <i>Guide to health privacy</i> (v 1.0, 6 September 2019) < <a href="https://oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/">https://oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/</a> >
<b>OIC</b>	Office of the Information Commissioner (Queensland)
<b>OIC Guideline: Applications by and for children (2017)</b>	Office of the Information Commissioner (Queensland), <i>Guidelines—Access and amendment: Applications by and for children</i> (5 June 2017) < <a href="https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/processing-applications/applications-by-and-for-children">https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/processing-applications/applications-by-and-for-children</a> >.
<b>OIC Guideline: Key privacy concepts—agreement and consent (2013)</b>	Office of the Information Commissioner (Queensland), <i>Guidelines—Privacy principles: Key privacy concepts—agreement and consent</i> (19 July 2013) < <a href="https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/key-privacy-concepts/key-privacy-concepts-agreement-and-consent">https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/key-privacy-concepts/key-privacy-concepts-agreement-and-consent</a> >
<b>OIC Guideline: Privacy and children (2012)</b>	Office of the Information Commissioner (Queensland), <i>Guidelines—Privacy principles: Privacy and children</i> (30 July 2012) < <a href="https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-children">https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-children</a> >

<b>OIC, Information Sheet: Camera surveillance, video, and audio recording—a community guide (2019)</b>	Office of the Information Commissioner (Queensland), <i>Information Sheet—Privacy principles: Camera surveillance, video, and audio recording—a community guide</i> (24 September 2019) < <a href="https://www.oic.qld.gov.au/guidelines/for-community-members/Information-sheets-privacy-principles/camera-surveillance,-video,-and-audio-recording-a-community-guide">https://www.oic.qld.gov.au/guidelines/for-community-members/Information-sheets-privacy-principles/camera-surveillance,-video,-and-audio-recording-a-community-guide</a> >
<b>overt surveillance</b>	Surveillance that is done in such a way that the subject of surveillance is aware that the surveillance is occurring, for example, where the surveillance device is not concealed.
<b>participant monitoring</b>	In general terms, the use of a listening device or an optical surveillance device by a party to a private conversation or a private activity to record the conversation or activity without the knowledge or consent of the other party or parties.
<b>PPRA</b>	<i>Police Powers and Responsibilities Act 2000</i> (Qld)
<b>Privacy Act</b>	<i>Privacy Act 1988</i> (Cth)
<b>QAI</b>	Queensland Advocacy Incorporated
<b>QCAT</b>	Queensland Civil and Administrative Tribunal
<b>QCCL</b>	Queensland Council for Civil Liberties
<b>QDS (2018)</b>	Queensland Government, <i>Queensland Drones Strategy</i> (June 2018)
<b>QDS Consultation Paper (2017)</b>	Queensland Government, 'Queensland Drones Strategy' (Consultation Paper, Department of the Premier and Cabinet, August 2017)
<b>QGCI</b>	Queensland Government Chief Information Office, Department of Housing and Public Works
<b>QLRC Consultation Paper No 77 (2018)</b>	Queensland Law Reform Commission, <i>Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies</i> , Consultation Paper, WP No 77 (December 2018)
<b>QLS</b>	Queensland Law Society
<b>Review of the RTI Act and IP Act (2017)</b>	Department of Justice and Attorney-General (Queensland), 'Report on the review of the <i>Right to Information Act 2009</i> and <i>Information Privacy Act 2009</i> ' (October 2017)
<b>SA Legislative Review Committee Report (2013)</b>	Legislative Review Committee, Parliament of South Australia, <i>Report of the Legislative Review Committee into Issues Relating to Surveillance Devices</i> (November 2013)
<b>surveillance devices legislation</b>	Legislation regulating the use of surveillance devices in each Australian jurisdiction, namely: <ul style="list-style-type: none"> <li>• <i>Invasion of Privacy Act 1971</i> (Qld)</li> <li>• <i>Listening Devices Act 1992</i> (ACT)</li> <li>• <i>Surveillance Devices Act 2007</i> (NSW) and <i>Surveillance Devices Regulation 2014</i> (NSW)</li> </ul>

	<ul style="list-style-type: none"> <li>• <i>Surveillance Devices Act</i> (NT) and <i>Surveillance Devices Regulations</i> (NT)</li> <li>• <i>Surveillance Devices Act 2016</i> (SA) and <i>Surveillance Devices Regulations 2017</i> (SA)</li> <li>• <i>Listening Devices Act 1991</i> (Tas) and <i>Listening Devices Regulations 2014</i> (Tas)</li> <li>• <i>Surveillance Devices Act 1999</i> (Vic) and <i>Surveillance Devices Regulations 2016</i> (Vic)</li> <li>• <i>Surveillance Devices Act 1998</i> (WA) and <i>Surveillance Devices Regulations 1999</i> (WA)</li> </ul>
<b>use prohibitions</b>	The prohibitions under surveillance devices legislation against using (or installing, maintaining or attaching) a surveillance device for certain purposes.
<b>VLRC</b>	Victorian Law Reform Commission
<b>VLRC Report No 18 (2010)</b>	Victorian Law Reform Commission, <i>Surveillance in Public Places</i> , Report No 18 (June 2010)
<b>VLRC Consultation Paper No 7 (2009)</b>	Victorian Law Reform Commission, <i>Surveillance in Public Places</i> , Consultation Paper No 7 (January 2009)
<b>VLRC Occasional Paper (2002)</b>	K Foord, <i>Defining Privacy</i> , Victorian Law Reform Commission, Occasional Paper (2002)
<b>VLRC Information Paper (2001)</b>	Victorian Law Reform Commission, <i>Privacy Law: Options for Reform</i> , Information Paper (July 2001)

\* Except where otherwise indicated, references to legislation in this Report are references to Queensland legislation.

# Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>i</b>
<b>LIST OF RECOMMENDATIONS .....</b>	<b>ix</b>
<b>CHAPTER 1 .....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>1</b>
THE TERMS OF REFERENCE .....	1
The Consultation Paper .....	2
Submissions .....	2
The structure of this Report.....	3
TERMINOLOGY .....	4
<b>CHAPTER 2 .....</b>	<b>5</b>
<b>BACKGROUND .....</b>	<b>5</b>
SURVEILLANCE AND SURVEILLANCE DEVICE TECHNOLOGIES .....	5
PRIVACY .....	7
SURVEILLANCE DEVICES LEGISLATION .....	9
Queensland: <i>Invasion of Privacy Act 1971</i> .....	9
Other jurisdictions .....	11
Criminal penalties.....	16
Surveillance and law enforcement in Queensland.....	17
OTHER LAWS RELEVANT TO SURVEILLANCE AND PRIVACY .....	17
<b>CHAPTER 3 .....</b>	<b>19</b>
<b>A NEW APPROACH TO REGULATING THE USE OF SURVEILLANCE DEVICES ..</b>	<b>19</b>
INTRODUCTION .....	19
The need for new surveillance devices legislation in Queensland .....	20
THE COMMISSION'S APPROACH .....	21
Balancing surveillance and privacy .....	21
Consent .....	22
Exceptions for authorised use.....	22
Exceptions for justified and 'reasonably necessary' purposes .....	23
A criminal law and a civil law response .....	23
The draft Bill .....	23
ALTERNATIVE APPROACHES .....	24
RECOMMENDATION .....	28
<b>CHAPTER 4 .....</b>	<b>29</b>
<b>PRELIMINARY MATTERS .....</b>	<b>29</b>
THE APPLICATION OF THE DRAFT BILL.....	29
The application of the draft Bill to all persons .....	29
Relationship with other laws.....	29
THE DEFINITION OF SURVEILLANCE DEVICE AND RELATED DEFINITIONS .....	32
Approaches to the definition of surveillance device .....	32
Submissions .....	34
The Commission's view .....	37

THE DEFINITION OF CONSENT .....	42
The meaning of consent.....	42
Submissions .....	45
The Commission's view .....	47
RECOMMENDATIONS .....	51
 <b>CHAPTER 5 .....</b>	<b>55</b>
<b>CRIMINAL PROHIBITIONS ON THE USE OF SURVEILLANCE DEVICES .....</b>	<b>55</b>
INTRODUCTION .....	55
SURVEILLANCE DEVICES LEGISLATION .....	56
SUBMISSIONS.....	57
Prohibition on the use of a surveillance device for particular purposes.....	57
Criminal penalty.....	61
Exceptions to the prohibition on the use of a surveillance device .....	62
THE COMMISSION'S VIEW .....	78
The approach of the draft Bill .....	78
ELEMENTS OF THE USE PROHIBITIONS .....	79
Intention.....	79
Use, install or maintain surveillance devices .....	82
Prohibited uses.....	84
Private conversations and activities.....	86
Tracking devices and data surveillance devices.....	92
Parties .....	93
Consent.....	95
Criminal penalty.....	100
EXCEPTIONS TO THE USE PROHIBITIONS.....	101
Participant monitoring .....	102
Protection of lawful interests .....	103
Public interest.....	111
Safety and wellbeing .....	120
Location and retrieval of a lost or stolen vehicle or other thing.....	121
Authorised under another Act of the State or an Act of the Commonwealth .....	123
Prescribed circumstances .....	126
Security providers and insurance adjusters .....	127
Not for communication or publication to a person who is not a party .....	129
Lawful purpose.....	130
RECOMMENDATIONS .....	130
 <b>CHAPTER 6 .....</b>	<b>137</b>
<b>CRIMINAL PROHIBITIONS ON THE COMMUNICATION OR PUBLICATION OF SURVEILLANCE INFORMATION .....</b>	<b>137</b>
INTRODUCTION .....	137
SURVEILLANCE DEVICES LEGISLATION .....	138
Queensland .....	138
Other jurisdictions .....	140
SUBMISSIONS.....	143
Communication or publication prohibitions .....	143
Exceptions to the communication or publication prohibitions .....	144
THE COMMISSION'S VIEW .....	148
The approach of the draft Bill .....	148
ELEMENTS OF THE COMMUNICATION OR PUBLICATION PROHIBITIONS.....	149
Intention or knowledge .....	149

Surveillance information that the communication or publication prohibitions apply to.....	149
Consent .....	150
Criminal penalty.....	150
EXCEPTIONS TO THE COMMUNICATION OR PUBLICATION PROHIBITIONS .....	151
Communication or publication in legal proceedings.....	152
Communication or publication to protect that person's lawful interests .....	153
Communication or publication in the public interest.....	156
Communication or publication for safety and well-being .....	161
Communication or publication authorised under another Act or prescribed by regulation .....	162
Communication or publication by security providers and loss adjusters .....	163
Communication or publication to a person with a reasonable interest in the circumstances .....	164
Communication or publication in the performance of a duty.....	164
Communication or publication by a person who obtained knowledge other than by unlawful use of the device .....	166
Communication or publication to a party.....	166
RECOMMENDATIONS .....	167

<b>CHAPTER 7 .....</b>	<b>171</b>
<b>ANCILLARY MATTERS .....</b>	<b>171</b>
INTRODUCTION .....	171
OTHER PROHIBITIONS .....	171
Possession of records obtained from the prohibited use of surveillance devices .....	171
Possession, manufacture, supply or advertising of surveillance devices .....	173
Submissions .....	174
The Commission's view .....	175
USE OF A SURVEILLANCE DEVICE TO HARRASS, INTIMIDATE OR HINDER A PERSON .....	176
Submissions .....	178
The Commission's view .....	179
UNLAWFUL ENTRY OF DWELLING HOUSES .....	180
The Commission's view .....	181
CORPORATE OFFICER LIABILITY .....	181
Submissions .....	182
The Commission's view .....	183
ADMISSIBILITY OF EVIDENCE OBTAINED FROM THE UNLAWFUL USE OF A SURVEILLANCE DEVICE.....	183
Submissions .....	186
The Commission's view .....	186
NON-PUBLICATION ORDERS .....	187
The Commission's view .....	189
FORFEITURE ORDERS .....	190
Submissions .....	191
The Commission's view .....	191
RECOMMENDATIONS .....	192

<b>CHAPTER 8 .....</b>	<b>197</b>
<b>GENERAL OBLIGATIONS NOT TO INTERFERE WITH SURVEILLANCE PRIVACY OF INDIVIDUALS .....</b>	<b>197</b>
INTRODUCTION .....	197
SUBMISSIONS.....	197
APPROACHES IN OTHER JURISDICTIONS .....	199

Breach of a criminal prohibition as ground for a civil complaint.....	199
Breach of legislative principles as ground for a civil complaint.....	200
Separate civil 'tort' or cause of action .....	202
THE LEGISLATIVE CONTEXT IN QUEENSLAND .....	207
THE COMMISSION'S VIEW .....	207
ELEMENTS OF THE RECOMMENDED APPROACH .....	209
Statement and scope of the general obligations .....	209
Intention and knowledge .....	215
Consent .....	216
Exceptions .....	217
RECOMMENDATIONS .....	225

## **CHAPTER 9 ..... 229**

### **CIVIL COMPLAINTS PROCESS AND REMEDIES..... 229**

INTRODUCTION .....	229
SUBMISSIONS.....	229
Mediation or conciliation of complaints .....	229
Civil remedies.....	230
EXISTING PROVISIONS AND PROPOSALS .....	233
Other jurisdictions .....	234
Other legislation in Queensland .....	235
THE COMMISSION'S VIEW .....	239
ELEMENTS OF THE RECOMMENDED APPROACH .....	242
Making and referring complaints to the commissioner .....	242
Dealing with complaints .....	246
Mediation of complaints .....	250
Referral of complaints to tribunal .....	253
Enforcement of tribunal orders .....	259
RECOMMENDATIONS .....	260

## **CHAPTER 10 ..... 271**

### **A NEW REGULATOR ..... 271**

INTRODUCTION .....	271
SUBMISSIONS.....	271
An independent regulator .....	271
The regulator's functions and powers .....	276
EXISTING PROVISIONS AND PROPOSALS .....	278
Other jurisdictions .....	279
Other legislation in Queensland .....	283
THE COMMISSION'S VIEW .....	287
Which entity .....	287
ELEMENTS OF THE RECOMMENDED APPROACH .....	291
Establishment of the regulator .....	291
Functions and powers .....	293
Reporting requirements.....	299
Protections and offences.....	301
Review of decisions .....	303
RECOMMENDATIONS .....	303



<b>CHAPTER 11 .....</b>	<b>313</b>
<b>GENERAL MATTERS .....</b>	<b>313</b>
REGULATION-MAKING POWER .....	313
REVIEW OF ACT .....	313
CONSEQUENTIAL AMENDMENTS AND RELATED MATTERS .....	314
Acts referring to the <i>Invasion of Privacy Act 1971</i> .....	314
Statements relating to the use of an optical surveillance device .....	315
Sections 43(2)(c) and (e) and 45(2)(e) of the <i>Invasion of Privacy Act 1971</i> .....	316
RECOMMENDATIONS .....	317
 <b>APPENDIX A.....</b>	 <b>319</b>
<b>TERMS OF REFERENCE .....</b>	<b>319</b>
 <b>APPENDIX B.....</b>	 <b>323</b>
<b>LIST OF RESPONDENTS .....</b>	<b>323</b>
 <b>APPENDIX C.....</b>	 <b>325</b>
<b>COMPARATIVE GUIDE TO SURVEILLANCE DEVICES LEGISLATION.....</b>	<b>325</b>
 <b>APPENDIX D.....</b>	 <b>333</b>
<b>OTHER LAWS RELEVANT TO SURVEILLANCE AND PRIVACY .....</b>	<b>333</b>
 <b>APPENDIX E .....</b>	 <b>347</b>
<b>CIVIL SURVEILLANCE LAW REFORM REVIEWS AND OTHER INQUIRIES IN</b>	
<b>OTHER JURISDICTIONS.....</b>	<b>347</b>
 <b>APPENDIX F .....</b>	 <b>355</b>
<b>DRAFT SURVEILLANCE DEVICES BILL 2020.....</b>	<b>355</b>



# Executive Summary

## INTRODUCTION

[1] The Commission was asked to recommend whether Queensland should consider legislation to appropriately protect the privacy of individuals in the context of civil surveillance technologies.<sup>1</sup>

[2] Over time, surveillance device technologies have become increasingly sophisticated, accessible and affordable. Different surveillance devices capture different types of information, and may be used for different purposes. Whatever the purpose of their use, surveillance devices have the potential to impact on individual privacy.

[3] In Queensland, there is limited regulation of the use of surveillance devices. The *Invasion of Privacy Act 1971* regulates the use of a listening device to overhear, listen to, monitor or record private conversations, and the communication or publication of information obtained from such use. However, it does not extend to other types of surveillance devices. In contrast, in most other Australian jurisdictions, surveillance devices legislation regulates the use of listening devices, optical surveillance devices, tracking devices and, in some jurisdictions, data surveillance devices.

[4] In addition, surveillance devices legislation in Queensland and other jurisdictions does not provide a civil response to an unjustified interference with an individual's privacy caused by the use of a surveillance device.

[5] Other general laws, including information privacy legislation, the criminal law and some civil causes of action, offer only piecemeal and limited protection for the privacy of individuals in this context.

## THE COMMISSION'S APPROACH

[6] In view of the gaps and uncertainties in the current laws in Queensland that regulate the use of surveillance devices, there is a need for a more comprehensive legislative response to appropriately protect the privacy of individuals in relation to the use of surveillance devices in civil society.

[7] The Commission therefore recommends that the *Invasion of Privacy Act 1971* be repealed and replaced by new legislation which implements the Commission's recommendations in the form of the draft Surveillance Devices Bill 2020 (the 'draft Bill') in **Appendix F**.

[8] In developing its recommendations for the draft Bill, the Commission has been informed by a number of principles and considerations, including:

---

<sup>1</sup>

The terms of reference are set out in Appendix A. The terms of reference exclude Queensland's existing law regulating the use of surveillance devices for State law enforcement purposes and workplace surveillance from the review: see terms of reference, paras E–F.

- the importance of community expectations;
- the need to balance the protection of an individual's privacy and the justified use of surveillance devices;
- the importance of consent as an authorising concept:
  - if there is consent, the use of a surveillance device, or the communication or publication of information obtained from the use of a surveillance device, should be lawful;
  - in the absence of consent, the use, communication or publication should be unlawful unless an exception applies;
- that objective standards should form the basis for the justified use of surveillance devices in the absence of consent;
- that the regulation of surveillance devices should be practical, and include:
  - a criminal law response where the seriousness of a person's conduct in using a surveillance device justifies the intervention of the State in imposing criminal sanctions; and
  - a civil law response to promote the responsible use of surveillance devices in everyday contexts and to empower individuals whose privacy is affected to seek civil redress in appropriate circumstances;
- the desirability of reasonable consistency with surveillance devices legislation in other Australian jurisdictions; and
- that the operation of other laws regulating the use of surveillance devices should not be affected.

[9] The Commission also recognises that surveillance devices legislation may overlap with but has a different focus from legislation that regulates information privacy and data protection.

[10] An overview of the Commission's principal recommendations and corresponding provisions of the draft Bill is set out below.

## THE SCOPE AND PURPOSE OF THE DRAFT BILL

[11] The main purpose of the draft Bill is to provide for an individual's privacy to be protected from unjustified interference from the use, or the communication or publication of information obtained from the use, of surveillance devices (**cl 2(1)**).

[12] Consistently with the surveillance devices legislation in other Australian jurisdictions, the draft Bill adopts a 'recognised categories' approach to regulating surveillance devices. This approach takes into account that different types of devices give rise to different privacy concerns and considerations.

[13] For the purposes of the draft Bill, a ‘surveillance device’ is defined as a listening device, an optical surveillance device, a tracking device, a data surveillance device or a device that is a combination of two or more of those devices (**cl 6**).

## CRIMINAL PROHIBITIONS

### The use prohibitions

[14] The draft Bill contains four prohibitions on the use of a surveillance device (‘the use prohibitions’). Specifically, it provides that a person must not use, install or maintain:

- a listening device to listen to, monitor or record a private conversation, without the consent of each party to the conversation (**cl 18**);
- an optical surveillance device to observe, monitor or visually record a private activity, without the consent of each party to the activity (**cl 19**);
- a tracking device to find, monitor or record the geographical location of:
  - an individual, without the consent of the individual (**cl 20(1)**); or
  - a vehicle or other thing, without the consent of each person who owns, or is in lawful control of, the vehicle or thing (**cl 20(2)**); or
- a data surveillance device to access, monitor or record information that is input into, output from or stored in a computer, without the consent of each person who owns, or is in lawful control of, the computer (**cl 21**).

[15] There are exceptions to the use prohibitions. It is not an offence for a person to use, install or maintain a surveillance device if:

- use of the device is reasonably necessary to protect the lawful interests of that person, or of another person who has authorised the person to use the surveillance device on their behalf (**cl 22**);
- use of the device is reasonably necessary in the public interest (**cl 23**);
- it is to obtain evidence of, or information about, a serious threat to the life, health safety or wellbeing of an individual, or a serious threat of substantial damage to property, if the person believes, on reasonable grounds, it is necessary for the device to be used immediately to obtain the evidence or information (**cl 24**); or
- the use, installation or maintenance is authorised under another Act of the State or an Act of the Commonwealth, or in circumstances prescribed by regulation (**cl 26**).

[16] There is an additional exception for the use of a surveillance device to locate a lost or stolen vehicle or other thing (**cl 25**).

[17] In contrast to the *Invasion of Privacy Act 1971*, the draft Bill does not generally permit participant monitoring; in the absence of consent, the use of

surveillance device should be unlawful unless an exception (for a specific purpose which justifies the use) applies.

### The communication or publication prohibitions

[18] The draft Bill contains three prohibitions on the communication or publication of information obtained from the use of a surveillance device ('the communication or publication prohibitions'). Specifically, it prohibits a person from communicating or publishing surveillance information<sup>2</sup> about:

- a private conversation or a private activity if the person knows, or ought reasonably to know, the information is surveillance information, and the person does not have the consent of each party to the conversation or activity to communicate or publish the information (**cl 28**);
- the geographical location of an individual, a vehicle or another thing if the person knows, or ought reasonably to know, the information is surveillance information, and the person does not have the consent of the following person or persons to communicate or publish the information:
  - for information about the location of an individual—that individual;
  - for information about the location of a vehicle or other thing—each person who owns, or is in lawful control of, the vehicle or thing (**cl 29**); or
- information that is input into, output from or stored in a computer, if the person knows, or ought reasonably to know, the information is surveillance information, and the person does not have the consent of each person who owns, or is in lawful control of, the computer to communicate or publish the information (**cl 30**).

[19] There are exceptions to the communication or publication prohibitions. It is not an offence for a person to communicate or publish surveillance information if the communication or publication is:

- in a legal proceeding (**cl 31(1)(a)**);
- reasonably necessary to protect the lawful interests of the person, or of another person who has authorised the person to communicate or publish the information on their behalf (**cl 31(1)(b)**);
- reasonably necessary in the public interest (**cl 31(1)(c)**);
- reasonably necessary to lessen or prevent a serious threat to the life, health, safety or wellbeing of an individual, or of substantial damage to property (**cl 31(1)(d)**); or

---

<sup>2</sup> Under the draft Bill, 'surveillance information' is defined to mean information obtained, directly or indirectly, using a surveillance device (**cl 14**).

- authorised under another Act of the State or an Act of the Commonwealth, or in circumstances prescribed by regulation (**cl 31(1)(e), (f)**).

[20] In addition, a person does not contravene the communication or publication prohibitions if the use of a surveillance device to obtain the surveillance information the subject of the communication or publication was authorised under another Act (**cl 31(2)**).

[21] The maximum penalty for a contravention of the use prohibitions or the communication or publication prohibitions is 60 penalty units (\$8007) or three years imprisonment.

### **Prohibition on possessing surveillance information**

[22] The draft Bill also makes it an offence for a person, without the consent of each relevant person, to possess information that the person knows is surveillance information obtained in contravention of a use prohibition (**cl 27(1)**).

[23] This offence does not apply if the person possesses the information in relation to proceedings for an offence against the draft Bill, or because the information was communicated to the person or published in a way that does not contravene the draft Bill (**cl 27(2)**). The maximum penalty for a contravention of the prohibition on possessing surveillance information is 20 penalty units (\$2669) or one year's imprisonment.

### **Ancillary orders relating to the criminal prohibitions**

[24] The court is empowered to make ancillary orders relating to proceedings for a contravention of the criminal prohibitions:

- in a proceeding for an offence against Part 2 of the legislation, the court may, at any time during the proceeding and if it considers it necessary in the interests of justice, make an order prohibiting the publication of evidence before the court, other than in the way and to the persons stated in the order (**cl 32**);
- if a person is convicted of an offence against the legislation, the court may order that:
  - a surveillance device used in connection with the commission of the offence, or a document, device or other thing that contains or stores related information (that is, information to which the offence relates, or obtained using a surveillance device to which the offence relates) is forfeited to the State; or
  - related information be destroyed (**cl 33**).

### **GENERAL OBLIGATIONS NOT TO INTERFERE WITH SURVEILLANCE PRIVACY OF INDIVIDUALS**

[25] To address situations where a person's conduct interferes with an individual's surveillance privacy, the draft Bill imposes a general obligation on a user

of a surveillance device not to use the device in a way that interferes with an individual's surveillance privacy (where the individual has a reasonable expectation of surveillance privacy and has not consented to such use) (**cl 36**). A similar general obligation applies in relation to the communication or publication of surveillance information (**cl 37**).

[26] In this context, 'surveillance privacy', of an individual, means:

- in relation to a particular use of a surveillance device—the individual is not the subject of surveillance from that use of a surveillance device; or
- in relation to surveillance information obtained when the individual was the subject of surveillance—the surveillance information is not communicated or published (**cl 34**).

[27] A 'reasonable expectation', of surveillance privacy for an individual, means that the individual is reasonably entitled to expect surveillance privacy in relation to a particular use of a surveillance device, or in relation to surveillance information obtained when the individual was the subject of surveillance (**cl 34**). Only those expectations that are reasonable in the circumstances will fall within the scope of the general obligations.

[28] The matters that are relevant for deciding whether an individual has a reasonable expectation of surveillance privacy include, but are not limited to:

- the individual's location when the surveillance device is used;
- the subject matter of the use, or of the surveillance information;
- the type of device used;
- the nature and purpose of the use, communication or publication;
- the nature and extent of any notice given about the use;
- whether the individual has an opportunity to avoid the surveillance; and
- the individual's attributes and conduct (**cl 35**).

[29] There are exceptions to the general obligation provisions. A person does not contravene a general obligation if the use, communication or publication is:

- authorised or required by law, or by an order or process of a court or tribunal;
- incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property, including to prosecute or defend a civil or criminal proceeding; or
- reasonably necessary in the public interest and the relevant public interest outweighs the interference with the individual's surveillance privacy (**cl 38**).



## CIVIL COMPLAINTS PROCESS AND REMEDIES

[30] The draft Bill provides a civil mechanism for the resolution of a complaint about an alleged contravention of a general obligation made by or for an individual who is the subject of the alleged contravention (a ‘surveillance device complaint’) (**cl 39**).

[31] The Commission recommends a three-stage approach for the resolution of a surveillance device complaint (**cll 39–65**):

- a complaint may be made to the Surveillance Devices Commissioner (established under the legislation) for mediation;
- an unresolved complaint may be referred to QCAT for hearing and decision; and,
- if appropriate, QCAT may order remedial relief (including an order that the respondent must not repeat or continue a stated act or practice, or must compensate the complainant for loss or damage suffered because of the respondent’s act or practice by engaging in a stated act or practice or paying an amount of not more than \$100 000).

[32] These provisions have been generally modelled on the mechanism for resolving privacy complaints under the *Information Privacy Act 2009*, with appropriate modifications.

## A NEW REGULATOR

[33] The Commission recommends the establishment of a new independent regulator—the Surveillance Devices Commissioner—and a Surveillance Devices Commission.

[34] In addition to dealing with surveillance device complaints, the Surveillance Devices Commissioner will provide an avenue for education, expert advice and monitoring and best practice guidance to promote community understanding and encourage compliance with the legislation.

[35] Accordingly, the Surveillance Devices Commissioner’s functions include:

- receiving surveillance device complaints and dealing with them under the legislation (**cl 72**);
- providing guidance (including, promoting understanding of and compliance with the general obligations and the operation of the legislation, and providing best practice for the use of surveillance devices and the communication or publication of surveillance information, in a way that respects individuals’ privacy) (**cl 73**);
- undertaking research, providing advice and monitoring particular matters, including research about whether the legislation is achieving its purpose, how surveillance devices and surveillance device technologies are used in civil society and developments in surveillance device technology, and identifying and commenting on any issues arising in relation to those matters (**cl 74**);

- examining the practices of relevant entities (including local and State government agencies and other entities performing functions of a public nature, and private sector organisations or individuals who regularly or routinely use or publish information from surveillance devices)<sup>3</sup> to monitor their compliance with the legislation (**cl 75**).

[36] The Commission also recommends reporting requirements relating to the Surveillance Device Commissioner's functions to ensure transparency, integrity and accountability (**cII 84–85**).

## PROTECTIONS AND OFFENCES

[37] To ensure the effective operation of the Surveillance Devices Commissioner's functions, the Commission recommends a small number of standard protective provisions (including protection from civil liability) and offences relating to the actions of and dealings with the Surveillance Devices Commissioner (**cl 88–92**).

## GENERAL MATTERS

[38] The Commission recommends that the Minister be required to complete a review of the effectiveness of the legislation within 5 years after its commencement. The review must consider:

- whether the legislation is achieving its purpose;
- how surveillance devices and surveillance device technologies are used in civil society;
- developments in surveillance device technology; and
- whether the legislation should be amended to provide for new types of surveillance devices or new uses of surveillance devices and surveillance devices technologies in civil society (**cl 95**).

---

<sup>3</sup>

This monitoring function does not apply, however, to the Queensland Police Service, the Crime and Corruption Commission or another entity to the extent its practices relate to enforcing a State law.

# List of Recommendations

## CHAPTER 3: A NEW APPROACH TO REGULATING THE USE OF SURVEILLANCE DEVICES

- 3-1 The *Invasion of Privacy Act 1971* should be repealed, and replaced by new legislation which implements the Commission's recommendations in the form of the draft Bill.

*[See Surveillance Devices Bill 2020 cl 96]*

## CHAPTER 4: PRELIMINARY MATTERS

### Application of the Act

- 4-1 The draft Bill should provide that the legislation binds all persons, including the State. The provision should also make it clear that the State cannot be prosecuted for an offence against the legislation.

*[See Surveillance Devices Bill 2020 cl 3]*

- 4-2 The draft Bill should not affect—

- (a) the operation of the *Information Privacy Act 2009*; or
- (b) the operation of another law regulating the use of surveillance devices.

*[See Surveillance Devices Bill 2020 cl 4(a), (b)]*

### Definition of 'surveillance device' and related definitions

- 4-3 The draft Bill should define 'surveillance device' as:

- (a) a listening device, an optical surveillance device, a tracking device, a data surveillance device; or
- (b) a device that is a combination of any two or more of those devices.

*[See Surveillance Devices Bill 2020 cl 6]*

- 4-4** The draft Bill should define ‘listening device’ as a device that is capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation. However, it should expressly exclude a hearing aid or a similar device used by an individual with impaired hearing.

*[See Surveillance Devices Bill 2020 cl 7]*

- 4-5** The draft Bill should define ‘optical surveillance device’ as a device capable of being used to observe, monitor or visually record an activity. However, it should expressly exclude spectacles, contact lenses or a similar device used by an individual with impaired vision.

*[See Surveillance Devices Bill 2020 cl 8]*

- 4-6** The draft Bill should define ‘tracking device’ as a device capable of being used to find, monitor or record the geographical location of an individual, vehicle or other thing.

*[See Surveillance Devices Bill 2020 cl 9]*

- 4-7** The draft Bill should define ‘data surveillance device’ as a device or program capable of being used to access, monitor or record information that is input into, output from, or stored in a computer.

*[See Surveillance Devices Bill 2020 cl 10]*

- 4-8** The draft Bill should define ‘computer’ as an electronic device for storing and processing information.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘computer’)]*

- 4-9** The draft Bill should define ‘surveillance information’ as information obtained, directly or indirectly, using a surveillance device.

*[See Surveillance Devices Bill 2020 cl 14]*

- 4-10** The draft Bill should define ‘information’ to include:

- (a) a record in any form; and
- (b) a document.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘information’)]*

**Definition of consent**

**4-11** The draft Bill should define ‘consent’ as express or implied consent.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘consent’)]*

**CHAPTER 5: CRIMINAL PROHIBITIONS ON THE USE OF SURVEILLANCE DEVICES****Definitions**

**5-1** The draft Bill should define ‘private conversation’ as:

- (a) Words spoken by an individual are a private conversation if the words are spoken in circumstances that may reasonably be taken to indicate that—

  - (i) for words not spoken to anyone else—the individual does not want anyone else to listen to the words; or
  - (ii) for words spoken to another individual, or other individuals—the individual, or at least one of the individuals to whom the words are spoken, does not want the words to be listened to by anyone other than—

    - (A) the individual speaking the words; and
    - (B) the individuals to whom the words are spoken; and
    - (C) any other individual who has the consent of all of the individuals mentioned in subparagraphs (A) and (B).
- (b) However, a private conversation does not include words spoken by an individual in circumstances in which the individual, and all of the individuals to whom the words are spoken, ought reasonably to expect that someone else may listen to, monitor or record the words.

*[See Surveillance Devices Bill 2020 cl 11]*

**5-2 The draft Bill should define ‘private activity’ as:**

- (a) An activity is a private activity if it is carried out in circumstances that may reasonably be taken to indicate that—**
  - (i) for an activity carried out by one individual—the individual does not want anyone else to observe the activity; or**
  - (ii) for an activity carried out by two or more individuals—at least one of the individuals does not want the activity to be observed by anyone other than—**
    - (A) the individuals carrying out the activity; and**
    - (B) any other individual who has the consent of all of the individuals carrying out the activity.**
- (b) However, a private activity does not include an activity carried out by one or more individuals in circumstances in which all of the individuals carrying out the activity ought reasonably to expect that someone else may observe, monitor or visually record the activity.**

*[See Surveillance Devices Bill 2020 cl 12]*

**5-3 The draft Bill should define ‘party’ as:**

- (a) Each of the following is a party to a private conversation—**
  - (i) an individual who speaks, or is spoken to, during the conversation;**
  - (ii) an individual who listens to the conversation with the consent of all of the individuals mentioned in paragraph (i).**
- (b) Each of the following is a party to a private activity—**
  - (i) an individual carrying out the activity;**
  - (ii) an individual who observes the activity with the consent of all of the individuals mentioned in paragraph (i).**

*[See Surveillance Devices Bill 2020 cl 13]*

**5-4 The draft Bill should explain that, in the legislation, a reference to installing a surveillance device includes doing anything to, or in relation to, a device to enable it to be used as a surveillance device.**

*[See Surveillance Devices Bill 2020 cl 15]*

**5-5** The draft Bill should define ‘maintain’, in relation to a surveillance device, to include:

- (a) adjust, relocate, repair or service the device; and
- (b) replace a faulty device.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘maintain’)]*

**5-6** The draft Bill should explain that a reference to a person who owns a vehicle, computer or other thing does not include a person (an ‘excluded owner’) who owns the vehicle, computer or other thing if:

- (a) another person has the use or control of the vehicle, computer or other thing under a credit agreement, hiring agreement, hire-purchase agreement, leasing agreement or another similar agreement; and
- (b) under the agreement, the excluded owner is not entitled to immediate possession of the vehicle, computer or other thing.

*[See Surveillance Devices Bill 2020 cl 16]*

#### **Prohibitions on the use, installation or maintenance of surveillance devices**

**5-7** The draft Bill provide that a person must not use, install or maintain a listening device to listen to, monitor or record a private conversation without the consent of each party to the conversation.

*[See Surveillance Devices Bill 2020 cl 18]*

**5-8** The draft Bill should provide that a person must not use, install or maintain an optical surveillance device to observe, monitor or visually record a private activity without the consent of each party to the activity.

*[See Surveillance Devices Bill 2020 cl 19]*

**5-9** The draft Bill should provide that a person must not use, install or maintain a tracking device to find, monitor or record the geographical location of:

- (a) an individual without the consent of the individual; or
- (b) a vehicle or other thing without the consent of each person who owns, or is in lawful control of, the vehicle or thing.

*[See Surveillance Devices Bill 2020 cl 20]*

- 5-10** The draft Bill should provide that a person must not use, install or maintain a data surveillance device to access, monitor or record information that is input into, output from or stored in a computer without the consent of each person who owns, or is in lawful control of, the computer.

*[See Surveillance Devices Bill 2020 cl 21]*

- 5-11** The draft Bill should provide that a person who contravenes a prohibition in Recommendations 5-7 to 5-10 commits an offence, which is punishable by a maximum penalty of 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cll 18, 19, 20, 21]*

**Exceptions to the prohibitions on the use, installation or maintenance of surveillance devices**

- 5-12** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if use of the device is reasonably necessary to protect the lawful interests of:

- (a) the person; or
- (b) if another person has authorised the person to use the surveillance device on the other person's behalf—the other person.

*[See Surveillance Devices Bill 2020 cl 22]*

- 5-13** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if use of the device is reasonably necessary in the public interest.

*[See Surveillance Devices Bill 2020 cl 23(1)]*

- 5-14** For the purposes of Recommendation 5-13, in deciding whether the use of a surveillance device is reasonably necessary in the public interest, a court must consider the following matters as they existed when the person used, installed or maintained the device:

- (a) the subject matter of the use of the device;
- (b) the information that the person reasonably expected would be obtained from the use of the device;
- (c) the purpose for which the person intended to use information that the person reasonably expected would be obtained from the use of the device;



- (d) the nature of the public interest that arose in the circumstances;
- (e) whether the public interest could have been served in another reasonable way;
- (f) the extent to which the use, installation or maintenance of the device affected, or was likely to affect, the privacy of an individual;
- (g) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

*[See Surveillance Devices Bill 2020 cl 23(2)]*

- 5-15 The draft Bill should provide that a person who uses, installs or maintains a surveillance device to obtain evidence of, or information about, a serious threat does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the person believes, on reasonable grounds, it is necessary for the device to be used immediately to obtain the evidence or information.

*[See Surveillance Devices Bill 2020 cl 24(1)]*

- 5-16 For the purposes of Recommendation 5-15, the draft Bill should define the term ‘serious threat’ to mean:

- (a) a serious threat to the life, health, safety or wellbeing of an individual; or
- (b) a serious threat of substantial damage to property.

*[See Surveillance Devices Bill 2020 cl 24(2)]*

- 5-17 The draft Bill should provide that a person who uses a surveillance device to locate a vehicle or other thing does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the person:

- (a) is not in possession or control of the vehicle or thing; and
- (b) believes, on reasonable grounds, that the vehicle or thing is lost or stolen; and
- (c) is an owner of the vehicle or thing or, before the vehicle or thing was lost or stolen, was in lawful control of it.

*[See Surveillance Devices Bill 2020 cl 25]*

**5-18** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the use, installation or maintenance is:

- (a) authorised under another Act of the State or an Act of the Commonwealth; or
- (b) in circumstances prescribed by regulation.

*[See Surveillance Devices Bill 2020 cl 26]*

## **CHAPTER 6: CRIMINAL PROHIBITIONS ON THE COMMUNICATION OR PUBLICATION OF SURVEILLANCE INFORMATION**

### **Communicating or publishing surveillance information**

**6-1** The draft Bill should provide that a person must not communicate or publish surveillance information about a private conversation or private activity if the person:

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) the person does not have the consent of each party to the conversation or activity to communicate or publish the information.

*[See Surveillance Devices Bill 2020 cl 28]*

**6-2** The draft Bill should provide that a person must not communicate or publish surveillance information about the geographical location of an individual, a vehicle or another thing if the person:

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) the person does not have the consent of the following person or persons to communicate or publish the location:
  - (i) for information about the location of an individual—that individual;

- (ii) for information about the location of the vehicle or other thing—each person who owns, or is in lawful control of, the vehicle or thing.

*[See Surveillance Devices Bill 2020 cl 29]*

**6-3** The draft Bill should provide that a person must not communicate or publish surveillance information about information that is input into, output from or stored in a computer, if the person:

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) the person does not have the consent of each person who owns, or is in lawful control of, the computer to communicate or publish the information.

*[See Surveillance Devices Bill 2020 cl 30]*

**6-4** The draft Bill should provide that a person who contravenes a prohibition in Recommendations 6-1 to 6-3 above commits an offence, which is punishable by a maximum penalty of 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cll 28, 29 and 30]*

#### **Exceptions to the communication or publication prohibitions**

**6-5** The draft Bill should provide that a person does not commit an offence against the prohibitions in Recommendations 6-1 to 6-3 above if the communication or publication of surveillance information is:

- (a) in a legal proceeding; or
- (b) reasonably necessary to protect the lawful interests of:
  - (i) the person who is making the communication or publication; or
  - (ii) another person who has authorised the person making the communication or publication to do so on their behalf; or
- (c) reasonably necessary in the public interest; or
- (d) reasonably necessary to lessen or prevent a serious threat:
  - (i) to the life, health, safety or wellbeing of an individual; or
  - (ii) of substantial damage to property; or

(e) authorised under another Act of the State or an Act of the Commonwealth; or

(f) in circumstances prescribed by regulation.

*[See Surveillance Devices Bill 2020 cl 31(1)]*

**6-6** The draft Bill should provide that a person does not commit an offence against the prohibitions in Recommendations 6-1 to 6-3 above if the use of a surveillance device to obtain the surveillance information the subject of the communication or publication was authorised under another Act of the State or an Act of the Commonwealth.

*[See Surveillance Devices Bill 2020 cl 31(2)]*

**6-7** The draft Bill should provide that, for deciding whether the communication or publication of surveillance information is ‘reasonably necessary in the public interest’ for Recommendation 6-5(c) above, a court must consider the following matters as they existed when the person communicated or published the information:

- (a) the subject matter of the surveillance information;
- (b) the scope of the communication or publication;
- (c) the nature of the public interest that arose in the circumstances;
- (d) whether the public interest could have been served in another reasonable way;
- (e) the extent to which the communication or publication affected, or was likely to affect, the privacy of an individual; and
- (f) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

*[See Surveillance Devices Bill 2020 cl 31(3)]*

## CHAPTER 7: ANCILLARY MATTERS

### Possessing surveillance information

- 7-1** The draft Bill should provide that a person must not, without the consent of each relevant person, possess information that the person knows is surveillance information obtained in contravention of the use prohibitions in the legislation.

*[See Surveillance Devices Bill 2020 cl 27(1)]*

- 7-2** For the purposes of the offence in Recommendation 7-1 above, a ‘relevant person’, in relation to surveillance information, means—

- (a) if the surveillance information is about a private conversation obtained using a listening device—each party to the conversation;
- (b) if the surveillance information is about a private activity obtained using an optical surveillance device—each party to the activity;
- (c) if the surveillance information is about the geographical location of an individual obtained using a tracking device—the individual;
- (d) if the surveillance information is about the geographical location of a vehicle or other thing obtained using a tracking device—each person who owns, or is in lawful control of, the vehicle or thing; or
- (e) if the surveillance information is about the information input into, output from or stored in a computer obtained using a data surveillance device—each person who owns, or is in lawful control of, the computer.

*[See Surveillance Devices Bill 2020 cl 27(3)]*

- 7-3** However, for the purposes of the offence in Recommendation 7-1 above, a person does not commit an offence if the person possesses the information:

- (a) in relation to proceedings for an offence against the legislation; or
- (b) because it was communicated to the person, or published, in a way that does not contravene the legislation.

*[See Surveillance Devices Bill 2020 cl 27(2)]*

- 7-4** The draft Bill should provide that the maximum penalty for the offence in Recommendation 7-1 above is 20 penalty units or one year's imprisonment.

*[See Surveillance Devices Bill 2020 cl 27(1)]*

**Admissibility of evidence obtained from the use of a surveillance device**

- 7-5** The draft Bill should expressly state that it does not affect the power of a court to make a decision about the admissibility of information obtained using a surveillance device as evidence in a proceeding.

*[See Surveillance Devices Bill 2020 cl 4(c)]*

**Non-publication orders**

- 7-6** The draft Bill should provide that, in proceedings for an offence against Part 2 of the legislation (which deals with the criminal prohibitions), the court may, at any time during the proceeding and only if it considers it necessary in the interests of justice, make an order prohibiting the publication of evidence given before the court, other than in the way and to the persons stated in the order.

*[See Surveillance Devices Bill 2020 cl 32(1)–(4)]*

- 7-7** The draft Bill should provide that a person must not contravene an order made under the provision in Recommendation 7-6 above, unless the person has a reasonable excuse. The maximum penalty for such a contravention is 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cl 32(5)]*

**Forfeiture or destruction of surveillance device or information**

- 7-8** The draft Bill should provide that:

- (1)** if a person is convicted of an offence against the legislation, the court before which the person is convicted may make an order that:
  - (a)** a surveillance device used in connection with the commission of the offence is forfeited to the State;
  - (b)** a document, device or other thing that contains related information, or on which related information is stored, is forfeited to the State; or
  - (c)** related information be destroyed;
- (2)** before making an order for forfeiture or destruction, the court may require notice to be given to, and hear from, a person the court considers appropriate;

- (3) the power to order forfeiture or destruction should apply whether or not the surveillance device, document, device or thing to be forfeited, or related information to be destroyed, has been seized;
- (4) the court may also make any order that it considers appropriate to enforce the forfeiture;
- (5) the provision in Recommendation 7-8(1) above does not limit the court's powers under the *Penalties and Sentences Act 1992*, the *Criminal Proceeds Confiscation Act 2002* or another law;
- (6) when forfeited to the State, the surveillance device, document, device or thing becomes the State's property and may be dealt with as directed by the chief executive.

*[See Surveillance Devices Bill 2020 cl 33(1)–(6)]*

- 7-9 For the purposes of Recommendation 7-8 above, 'related information', for an offence, should be defined to mean 'information to which the offence relates, or obtained using a surveillance device to which the offence relates'.

*[See Surveillance Devices Bill 2020 cl 33(7)]*

## CHAPTER 8: GENERAL OBLIGATIONS NOT TO INTERFERE WITH SURVEILLANCE PRIVACY OF INDIVIDUALS

### General obligations not to interfere with surveillance privacy of individuals

- 8-1 The draft Bill should include civil provisions, separate from the criminal prohibitions in the legislation, that:
- (a) impose obligations on the use of, or the communication or publication of information obtained from the use of, a surveillance device, within the meaning of the draft Bill, to avoid interference with an individual's surveillance privacy; and
  - (b) form the basis for the complaints mechanism in Recommendations 9-1 to 9-32 below.

The civil provisions should have the features set out below.

*[See Surveillance Devices Bill 2020 pts 3 and 4]*

**Statement and scope of the general obligations**

**8-2 The draft Bill should provide that, if an individual has a reasonable expectation of surveillance privacy:**

- (a) a person must not use a surveillance device in a way that interferes with the individual's surveillance privacy; and**
- (b) a person must not communicate or publish the surveillance information in a way that interferes with the individual's surveillance privacy.**

*[See Surveillance Devices Bill 2020 cll 36(1)–(2) and 37(1)–(2)]*

**8-3 However, a person does not contravene a general obligation in Recommendation 8-2 above if:**

- (a) the individual concerned has consented to the surveillance device being used in that way or, relevantly, to the communication or publication; or**
- (b) the person did not know, and ought not reasonably to have known, that the particular use of the surveillance device or, relevantly, the communication or publication would interfere with the individual's surveillance privacy.**

*[See Surveillance Devices Bill 2020 cll 36(3) and 37(3)]*

**8-4 The draft Bill should provide that, for the purpose of this part of the draft Bill:**

- (a) 'surveillance privacy', of an individual, means:**
  - (i) in relation to a particular use of a surveillance device—the individual is not the subject of surveillance from that use of a surveillance device; or**
  - (ii) in relation to surveillance information obtained when the individual was the subject of surveillance—the surveillance information is not communicated or published; and**
- (b) 'reasonable expectation', of surveillance privacy for an individual, means the individual is reasonably entitled to expect surveillance privacy—**
  - (i) in relation to a particular use of a surveillance device; or,**
  - (ii) in relation to surveillance information obtained when the individual was the subject of surveillance.**

*[See Surveillance Devices Bill 2020 cl 34]*



**8-5** The draft Bill should provide that the matters that are relevant for deciding whether an individual has a reasonable expectation of surveillance privacy include (but are not limited to) the following:

- (a)** the individual's location when the surveillance device is used;
- (b)** the subject matter of the use, or of the surveillance information, including whether it is of an intimate, familial, health-related or financial nature;
- (c)** the type of device used;
- (d)** the nature and purpose of the use, communication or publication, including:
  - (i)** the extent to which the use, communication or publication targets the individual;
  - (ii)** whether the use is covert;
  - (iii)** in relation to the communication or publication, how the information is communicated or published; and
  - (iv)** whether the use, communication or publication contravenes a provision of an Act;
- (e)** the nature and extent of any notice given about the use;
- (f)** whether the individual has an opportunity to avoid the surveillance;
- (g)** the attributes and conduct of the individual, including:
  - (i)** the extent to which the individual has a public profile, invites or encourages publicity or shows a wish for privacy;
  - (ii)** the extent to which the individual is in a position of vulnerability;
  - (iii)** the nature of any relationship between the individual and the person using the surveillance device, or making the communication or publication; and
  - (iv)** the effect that the use, communication or publication is reasonably likely to have on the individual's health, safety or wellbeing.

*[See Surveillance Devices Bill 2020 cl 35]*

**Exceptions to the general obligations**

**8-6** A person does not contravene a general obligation in Recommendation 8-2 above if the person's use of a surveillance device or, relevantly, communication or publication of surveillance information:

- (a) is authorised or required by law or by an order or process of a court or tribunal;
- (b) is incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property, including to prosecute or defend a criminal or civil proceeding; or
- (c) is reasonably necessary in the public interest and the public interest outweighs the interference with the individual's surveillance privacy.

*[See Surveillance Devices Bill 2020 cl 38]*

**CHAPTER 9: CIVIL COMPLAINTS PROCESS AND REMEDIES****A complaints mechanism**

**9-1** The draft Bill should provide a mechanism for complaints about alleged contraventions of the general obligations in Recommendation 8-2 above ('surveillance device complaints') to the effect that:

- (a) complaints may be made to the Surveillance Devices Commissioner (the 'commissioner') established under Recommendation 10-2(b) below for mediation;
- (b) complaints not resolved by mediation may be referred to QCAT for hearing and decision; and
- (c) if appropriate, the tribunal may order remedial relief.

The complaints mechanism should have the features set out below.

*[See Surveillance Devices Bill 2020 pt 4, cl 39]*

**Making and referring complaints to the commissioner****9-2 A complaint under Recommendation 9-1 above:**

- (a) may be made to the commissioner:
  - (i) by an individual who is the subject of the alleged contravention;
  - (ii) by an agent of the individual; or
  - (iii) by a person authorised by the commissioner in writing to make the complaint for the individual; and
- (b) may be made under paragraph (a) jointly by or for two or more individuals.

*[See Surveillance Devices Bill 2020 cl 40]*

**9-3 A complaint may be referred to the commissioner by any of the following entities, if they consider that the complaint may also be a complaint under this legislation:**

- (a) the Information Commissioner, in relation to a complaint received under the *Information Privacy Act 2009*;
- (b) the Human Rights Commissioner, in relation to a complaint received under the *Human Rights Act 2019*;
- (c) the Ombudsman, in relation to a complaint received under the *Ombudsman Act 2001*;
- (d) the Health Ombudsman, in relation to a complaint received under the *Health Ombudsman Act 2013*; or
- (e) any other entity that has received the complaint in performing its functions under a law [including a law of another State or the Commonwealth].

*[See Surveillance Devices Bill 2020 cl 41, sch 1 (definitions of 'referral Act' and 'referral entity')]*

**9-4 A complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above must be in writing, state the complainant's name and contact details (including, for example, the complainant's postal or email address), state the respondent's name, address or other contact details if they are known, and include enough information to identify the alleged contravention to which the complaint relates.**

*[See Surveillance Devices Bill 2020 cl 42(1)]*

- 9-5** A complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above must be made or referred within six months after the alleged contravention that is the subject of the complaint came to the complainant's knowledge, or within a further period that the commissioner considers is reasonable in all the circumstances.

*[See Surveillance Devices Bill 2020 cl 43]*

- 9-6** For a complaint made to the commissioner by an individual under Recommendation 9-2 above, the commissioner must give reasonable help to the complainant to put the complaint in writing.

*[See Surveillance Devices Bill 2020 cl 42(2)]*

#### **Dealing with complaints**

- 9-7** The draft Bill should set out the way in which the commissioner is to deal with a complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above.

*[See Surveillance Devices Bill 2020 cl 44]*

#### **Preliminary notice and inquiries**

- 9-8** As soon as practicable after receiving a complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above, the commissioner must give a notice to the complainant and respondent stating:

- (a) the substance of the complaint;
- (b) the role of the commissioner in dealing with the complaint; and
- (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint.

The notice to the respondent must also require the respondent to advise the commissioner of the respondent's contact details, including, for example, the respondent's postal or email address.

*[See Surveillance Devices Bill 2020 cl 46]*

- 9-9** Where a complaint is made or referred to the commissioner under Recommendation 9-2 or 9-3 above, the commissioner may make preliminary inquiries about the complaint to decide how to deal with the complaint and, if the complaint does not include enough information to do so, to identify the respondent to the complaint.

*[See Surveillance Devices Bill 2020 cl 45]*

- 9-10 The Queensland Government should take steps to facilitate a memorandum of understanding between CASA and the commissioner about the sharing of information by CASA about registered owners and accredited flyers of drones for the purpose of complaints under the legislation.**

**Direction to protect privacy of complainant or respondent**

- 9-11 In dealing with a complaint, the commissioner may, by notice, direct a person not to communicate or publish information that identifies, or is likely to identify, the complainant or respondent to a complaint if the commissioner is satisfied on reasonable grounds that it is necessary to do so to protect the privacy of the complainant or respondent. Non-compliance with a direction, without reasonable excuse, should be an offence with a maximum penalty of 10 penalty units.**

*[See Surveillance Devices Bill 2020 cl 47]*

**Refusing to deal with a complaint**

- 9-12 The commissioner may refuse to deal with a complaint, or part of a complaint, if:**

- (a) the commissioner considers that:**
  - (i) the complaint does not comply with the requirements at Recommendation 9-4 above about the matters that must be stated in the complaint;**
  - (ii) there is a more appropriate course of action available under another law to deal with the subject of the complaint or part;**
  - (iii) the subject of the complaint or part has been appropriately dealt with by another entity; or**
- (b) the complaint or part was not made or referred to the commissioner within the time stated at Recommendation 9-5 above; or**
- (c) the complaint or part is frivolous, trivial, vexatious, misconceived or lacking in substance;**

*[See Surveillance Devices Bill 2020 cll 17, 48(1)]*

- 9-13 The commissioner may refuse to continue to deal with a complaint, or part of a complaint, under any of the grounds in Recommendation 9-12 above or if:**

- (a) the complainant does not comply with a reasonable request made by the commissioner in dealing with the complaint or part;**

- (b) the commissioner is satisfied on reasonable grounds that the complainant, without a reasonable excuse, has not cooperated in the commissioner's dealing with the complaint or part; or
- (c) the commissioner can not make contact with the complainant.

*[See Surveillance Devices Bill 2020 cll 17, 48(2)]*

**9-14 If the commissioner refuses to deal with a complaint or to continue dealing with a complaint under Recommendation 9-12 or 9-13 above:**

- (a) the commissioner must give notice of the refusal, with reasons, to the complainant and, unless the commissioner considers it is not necessary to do so in the circumstances, to the respondent; and
- (b) the complaint lapses, and the complainant cannot make a further complaint under this legislation about the same alleged contravention.

*[See Surveillance Devices Bill 2020 cll 49 and 50]*

**Referral of complaints to other entities**

**9-15 The commissioner may refer a complaint to another entity as follows, if it considers the complaint would be more appropriately dealt with by the other entity and if the complainant consents:**

- (a) if the subject of the complaint could be the subject of a privacy complaint under the *Information Privacy Act 2009*, the commissioner may refer the complaint to the Information Commissioner;
- (b) if the subject of the complaint could be the subject of a human rights complaint under the *Human Rights Act 2019*, the commissioner may refer the complaint to the Human Rights Commissioner;
- (c) if the subject of the complaint could be the subject of a complaint under the *Ombudsman Act 2001*, the commissioner may refer the complaint to the Ombudsman;
- (d) if the subject of the complaint could be the subject of a health service complaint under the *Health Ombudsman Act 2013*, the commissioner may refer the complaint to the Health Ombudsman.

*[See Surveillance Devices Bill 2020 cl 51(1)–(2)]*

**9-16** If the commissioner refers a complaint under Recommendation 9-15 above to another entity, the commissioner:

- (a) may, with the complainant's consent, give the entity information about the complaint obtained by the commissioner; and
- (b) must give notice of the referral, with reasons, to the complainant and, unless the commissioner considers it is not necessary to do so in the circumstances, to the respondent.

*[See Surveillance Devices Bill 2020 cl 51(3)–(4)]*

#### **Arrangements with other entities**

**9-17** The commissioner may enter into an arrangement with the Information Commissioner, the Human Rights Commissioner, the Ombudsman or the Health Ombudsman (a 'referral entity') to provide for:

- (a) the types of complaint under the legislation that the commissioner should refer to the referral entity (under Recommendation 9-15 above), and how the referral is made;
- (b) the types of complaint made under a referral Act that the referral entity should refer to the commissioner (under Recommendation 9-3 above), and how the referral is made;
- (c) dealing with a complaint or other matter under a referral Act that could also form the basis of a complaint under the legislation; or
- (d) cooperating in the performance by the commissioner and the referral entity in their respective functions to ensure the effective operation of the legislation and the referral entity's legislation.

*[See Surveillance Devices Bill 2020 cl 52, sch 1 (definitions of 'referral Act' and 'referral entity')]*

#### **Mediation of complaints**

**9-18** The draft Bill should specify that the purpose of mediation is to identify and clarify the issues in the complaint and to promote the resolution of the complaint in a way that is informal, quick and efficient.

*[See Surveillance Devices Bill 2020 cl 53]*

**9-19** The commissioner must try to mediate the complaint if:

- (a) in the commissioner's opinion, it is reasonably likely the complaint could be resolved by mediation; and
- (b) the commissioner does not:

- (i) refuse to deal with, or to continue to deal with, the complaint, under Recommendation 9-12 or 9-13 above; or
- (ii) refer the complaint to another entity under Recommendation 9-15 above.

*[See Surveillance Devices Bill 2020 cl 54(1)]*

**9-20** Where Recommendation 9-19 applies, the commissioner must give notice of the mediation to the complainant and respondent stating:

- (a) the substance of the complaint;
- (b) the powers the commissioner may exercise in trying to resolve the complaint by mediation; and
- (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint.

The notice to the respondent must also state that the respondent will have an opportunity to respond to the complaint in writing.

*[See Surveillance Devices Bill 2020 cl 55]*

**9-21** The commissioner may take the reasonable action the commissioner considers appropriate to try to resolve the complaint by mediation. Without limiting the steps the commissioner may take, the commissioner may:

- (a) ask the respondent to respond in writing to the complaint;
- (b) give the complainant a copy of the respondent's written response;
- (c) ask or direct the complainant or respondent to give the commissioner information relevant to the complaint, including by notice given under Recommendation 10-8(c) below;
- (d) make enquiries of, and discuss the complaint with, the complainant and respondent;
- (e) provide information to the complainant and respondent about the legislation and how it applies to the complaint; or
- (f) facilitate a meeting between the complainant and respondent.

*[See Surveillance Devices Bill 2020 cl 54(2)–(3), sch 1 (definition of 'information')]*



**Confidentiality of mediation**

**9-22** A person who is or has been the commissioner or a staff member of the commission must not disclose information coming to their knowledge during a mediation. However, this does not apply if the disclosure is made:

- (a) with the consent of the complainant and respondent to the complaint;
- (b) for the purpose of giving effect to the commissioner's complaints handling or reporting functions under the legislation;
- (c) for statistical purposes without identifying a person to whom the information relates;
- (d) for an inquiry or proceeding about an offence happening during the mediation;
- (e) for a proceeding founded on fraud alleged to be connected with, or to have happened during, the mediation; or
- (f) under a requirement imposed by an Act.

*[See Surveillance Devices Bill 2020 cl 56]*

**9-23** Evidence of anything said or done, or an admission made, in the course of the mediation of a complaint is admissible in a civil proceeding only if the complainant and respondent agree. However:

- (a) This provision does not apply to a mediated agreement filed with QCAT under Recommendation 9-25 below; and
- (b) A 'civil proceeding' for this provision does not include a civil proceeding founded on fraud alleged to be connected with, or to have happened, during the mediation.

*[See Surveillance Devices Bill 2020 cl 57]*

**Mediated agreement**

**9-24** If, after mediation, the complainant and respondent agree to resolve the complaint:

- (a) the agreement is not binding, as a 'mediated agreement', until it is written down, signed by the complainant and respondent and certified by the commissioner as the agreement signed by the parties in accordance with these requirements;
- (b) the commissioner must keep a copy of the mediated agreement.

*[See Surveillance Devices Bill 2020 cl 58]*

- 9-25** The complainant or respondent may file a copy of the mediated agreement prepared under Recommendation 9-24 above with QCAT.

*[See Surveillance Devices Bill 2020 cl 59(1)]*

- 9-26** If a mediated agreement is filed with QCAT under Recommendation 9-25 above, the tribunal may make orders necessary to give effect to the agreement if the tribunal is satisfied that:

- (a) the order is consistent with an order the tribunal may make under Recommendation 9-31 below or the QCAT Act; and
- (b) it is practicable to implement the order.

An order made by the tribunal under this provision is, and may be enforced as, an order of the tribunal under the QCAT Act.

*[See Surveillance Devices Bill 2020 cl 59(2)–(3)]*

**Referral of complaints to tribunal**

- 9-27** The draft Bill should provide that, if:

- (a) the commissioner does not:
  - (i) refuse to deal with, or to continue to deal with, the complaint, under Recommendation 9-12 or 9-13 above; or
  - (ii) refer the complaint to another entity under Recommendation 9-15 above; and
- (b) in the commissioner’s opinion, the complaint is unlikely to be resolved:
  - (i) by mediation of the complaint; or
  - (ii) despite attempts to mediate the complaint

the commissioner must give notice to the complainant and respondent that these provisions apply and that the commissioner will, if asked to do so by the complainant, refer the complaint to QCAT to decide.

*[See Surveillance Devices Bill 2020 cll 60 and 61]*

- 9-28** The complainant may, in writing to the commissioner, ask for the referral of the complaint to QCAT within 20 business days after receiving notice under Recommendation 9-27 above.

*[See Surveillance Devices Bill 2020 cl 62(1)]*

- 9-29** The commissioner must refer the complaint to QCAT within 20 business days after receiving a request made under Recommendation 9-28 above.

*[See Surveillance Devices Bill 2020 cl 62(2)]*

**Tribunal's jurisdiction and procedure**

- 9-30** Where a complaint is referred to QCAT under Recommendation 9-29 above:

- (a) the tribunal must exercise its original jurisdiction under the QCAT Act to hear and decide the complaint;
- (b) the complainant and respondent to the complaint are both parties to the proceeding;
- (c) the complainant is taken to be the applicant for the proceeding;
- (d) the respondent is taken to be the respondent for the proceeding;
- (e) subject to para (f) below, the rules and procedures applying to QCAT under the QCAT Act apply to the proceeding; and
- (f) for a hearing conducted by the tribunal in relation to the complaint, the tribunal is to be constituted by at least one legally qualified member.

*[See Surveillance Devices Bill 2020 cll 62(3), 63 and 64]*

- 9-31** After the hearing of a complaint referred to QCAT under Recommendation 9-29 above, the tribunal may make one or more of the following final decisions to decide the complaint:

- (a) an order that declares the respondent's use, communication or publication contravened a general obligation in Recommendation 8-2(a) or (b) above in relation to the complainant and, if QCAT considers appropriate, includes one or more of the following—
  - (i) an order that the respondent must not repeat or continue a stated act or practice;
  - (ii) an order that the respondent must compensate the complainant for loss or damage (including for injury to the complainant's feelings or humiliation) suffered because of the respondent's act or practice by:
    - (A) engaging in a stated act or practice; or
    - (B) paying the complainant a stated amount of not more than \$100 000;

- (b) an order dismissing the complaint, or part of the complaint;
- (c) an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

*[See Surveillance Devices Bill 2020 cll 17, 65(1)–(2)]*

- 9-32** An order made by the tribunal under Recommendation 9-31(a)(ii) above must state the reasonable time within which the relevant action must be taken.

*[See Surveillance Devices Bill 2020 cl 65(3)]*

### **Resourcing**

- 9-33** QCAT should be provided with any additional resources necessary to ensure the effective operation of the new jurisdiction conferred on the tribunal by the legislation.

## **CHAPTER 10: A NEW REGULATOR**

### **A new independent regulator**

- 10-1** There should be an independent regulator. For the purpose of the draft Bill, the independent regulator is established as a separate entity under Recommendation 10-2 below. If the independent regulator's functions were instead to be conferred on an existing entity, some of the recommended provisions would need appropriate modification. Whichever way the independent regulator is established, it should have the functions, powers and main features set out below.

*[See Surveillance Devices Bill 2020 pt 5]*

### **Establishment of the regulator**

- 10-2** There should be a Surveillance Devices Commission (the 'commission'). The commission:
- (a) is a statutory body for the *Financial Accountability Act 2009* and the *Statutory Bodies Financial Arrangements Act 1982*; and
  - (b) consists of the Surveillance Devices Commissioner appointed under Recommendation 10-3 below, and the staff of the commission employed under Recommendation 10-7 below.

*[See Surveillance Devices Bill 2020 cll 66, 67]*

**10-3 The Surveillance Devices Commissioner (the ‘commissioner’):**

- (a) is appointed by, and holds office on the terms and conditions decided by, the Governor in Council;
- (b) holds office for a term of not more than five years stated in the instrument of appointment and, if a person is reappointed as commissioner, may hold office for not more than ten years continuously; and
- (c) controls the commission.

*[See Surveillance Devices Bill 2020 cll 71, 77, 78(1)–(3)]*

**10-4 The draft Bill should also include standard provisions dealing with leave of absence as commissioner, vacancy in office, the grounds on which a person may be removed from office as commissioner, and the preservation of certain rights of public service employees. Other relevant provisions of general application in the *Acts Interpretation Act 1954* will also apply.**

*[See Surveillance Devices Bill 2020 cll 78(4), 79, 80, 81, 82]*

**10-5 The draft Bill should ensure the independence of the commissioner by providing that:**

- (a) in performing the commissioner’s functions, the commissioner must act independently, impartially and in the public interest; and
- (b) the commissioner is not subject to direction by any person about how the commissioner performs the commissioner’s functions.

Under Recommendation 10-12(d), (e), (f) and 10-16(b) below, the Minister may, however, request advice, assistance or an examination, and may require a report, about particular matters.

*[See Surveillance Devices Bill 2020 cll 69 and 70]*

**10-6 The commissioner may delegate to an appropriately qualified staff member of the commission the commissioner’s functions or powers under the legislation or another Act. Provisions of general application in the *Acts Interpretation Act 1954* will apply to the delegation.**

*[See Surveillance Devices Bill 2020 cl 93]*

**10-7 Staff of the commission:**

- (a) are employed under the *Public Service Act 2008*; and
- (b) are not subject to direction, other than from the commissioner or a person authorised by the commissioner, about how the commissioner's functions are to be performed.

*[See Surveillance Devices Bill 2020 cl 83]*

**Functions and powers****10-8 The draft Bill should provide the following in relation to the commissioner's general functions and powers:**

- (a) The commissioner has the functions and powers given by the legislation;
- (b) The commissioner has power to do all things that are necessary or convenient to be done to perform the commissioner's functions under the legislation; and
- (c) If the commissioner believes on reasonable grounds that a person may have information relevant to a complaint being dealt with by the commissioner or to another function being performed by the commissioner, the commissioner may, by written notice, ask or direct the person to give the information to the commissioner within a reasonable period.

*[See Surveillance Devices Bill 2020 cll 68 and 76(1)–(4)]*

**10-9 The commissioner's functions include receiving and dealing with complaints under Recommendations 9-1 to 9-29 above. There should be a clear administrative division, supported by formal policies and procedures, between the commissioner's complaints handling and mediation functions and the other functions of the commissioner.**

*[See Surveillance Devices Bill 2020 cl 72]*

**10-10 The commissioner's guidance functions include:**

- (a) promoting understanding of and compliance with the legislation, including the general obligations in Recommendation 8-2 above;
- (b) providing information and guidance about the operation of the legislation;
- (c) providing education and training about the legislation, including the general obligations in Recommendation 8-2 above and the lawful use of surveillance devices;

- (d) issuing guidelines about any matter related to the commissioner's functions, including guidelines on any of the following matters:**
  - (i) how the legislation applies;**
  - (ii) how an exception in Recommendation 5-12 to 5-18 or 6-5 to 6-7 above applies, including examples;**
  - (iii) best practice for the use of surveillance devices, and the communication or publication of surveillance information, in a way that respects individuals' privacy; and**
  - (iv) making, referring and dealing with complaints under Recommendation 9-1 above; and**
- (e) giving information and reasonable help to complainants and respondents in relation to their complaints and the processes under the legislation.**

*[See Surveillance Devices Bill 2020 cl 73(1)]*

**10-11 The draft Bill should additionally provide that the guidelines issued under Recommendation 10-10(d) above must be published on the commissioner's website.**

*[See Surveillance Devices Bill 2020 cl 73(2)]*

**10-12 The commissioner's research, advice and monitoring functions include:**

- (a) undertaking or commissioning research to monitor:**
  - (i) whether the legislation is achieving its purpose;**
  - (ii) how surveillance devices and surveillance device technologies are used in civil society;**
  - (iii) developments in surveillance device technology;**
- (b) identifying and commenting on any issues relating to the use of surveillance devices in civil society, and the communication or publication of surveillance information;**
- (c) identifying and commenting on legislative and administrative changes that would improve the operation of the legislation;**
- (d) on request of the Minister or on the commissioner's own initiative, advising the Minister about matters relevant to the operation and administration of the legislation;**
- (e) on request of the Minister, assisting the Minister to review the legislation under Recommendation 11-2 below; and**

- (f) on request of the Minister, examining other Acts and proposed legislation to determine whether they are, or would be, consistent with the purpose of the legislation and the general obligations in Recommendation 8-2 above.

*[See Surveillance Devices Bill 2020 cl 74]*

**10-13** The commissioner's compliance monitoring functions include examining—on the commissioner's own initiative or otherwise—the practices of relevant entities, in relation to the following matters, to monitor whether the practices comply with the legislation:

- (a) how the entities use surveillance devices, and communicate or publish surveillance information;
- (b) the surveillance device, and communication or publication, technologies used by the entities; and
- (c) the programs, policies and procedures of the entities in relation to each of the matters in paragraphs (a) and (b).

*[See Surveillance Devices Bill 2020 cl 75(1)]*

**10-14** For the purpose of Recommendation 10-13 above:

- (a) 'relevant entity' means:
  - (i) a 'public entity' within the meaning of the *Human Rights Act 2019*;
  - (ii) an entity with an annual turnover of more than \$5 million for the current or previous financial year;
  - (iii) an entity that regularly or routinely uses a surveillance device, or communicates or publishes surveillance information;
  - (iv) an entity that uses a surveillance device to monitor crowds in places that are open to or used by the public, whether or not on the payment of a fee; and
  - (v) another entity prescribed by regulation.
- (b) 'relevant entity' does not include an entity to the extent its practices relate to enforcing a law of the State, including, for example, the Queensland Police Service or the Crime and Corruption Commission.

*[See Surveillance Devices Bill 2020 cl 75(2)]*



**Reporting requirements**

**10-15** In addition to the annual financial reporting requirements that will apply under the *Financial Accountability Act 2009*, the draft Bill should provide that:

- (a) as soon as practicable after the end of each financial year, the commissioner must give the Minister an annual report about the operation of the legislation;
- (b) without limiting paragraph (a), the annual report must include information for the financial year about the following matters:

  - (i) the number of complaints made or referred to the commissioner;
  - (ii) the types of complaints made or referred to the commissioner, including:

    - (A) the categories of entities to which the complaints relate;
    - (B) the uses of surveillance devices to which the complaints relate;
    - (C) the provisions of Recommendation 8-2 ff above to which the complaints relate;
  - (iii) the outcome of complaints made or referred to the commissioner, including:

    - (A) the number of complaints the commissioner refused to deal with, or to continue to deal with, and the grounds for refusing under Recommendations 9-12 and 9-13 above;
    - (B) the number and type of complaints referred to another entity under Recommendation 9-15 above;
    - (C) the number and type of complaints resolved by the commissioner by mediation under Recommendation 9-19 above;
    - (D) the number and type of complaints referred to QCAT under Recommendation 9-29 above;
  - (iv) the outcome of complaints referred to QCAT;
  - (v) another matter prescribed by regulation.

- (c) the Minister must table a copy of the annual report in the Legislative Assembly within 14 sitting days after receiving the report.

*[See Surveillance Devices Bill 2020 cl 84]*

**10-16 The draft Bill should also provide that:**

- (a) the commissioner may at any time prepare a report about a matter relevant to the performance of the commissioner's functions under the legislation and give the report to the Minister;
- (b) the commissioner must, if asked by the Minister, prepare a report about a matter mentioned in paragraph (a) and give the report to the Minister as soon as practicable after it is prepared; and
- (c) the Minister must table a copy of a report given to the Minister under paragraph (a) or (b) in the Legislative Assembly within 14 sitting days after receiving the report.

*[See Surveillance Devices Bill 2020 cl 85]*

**10-17 The draft Bill should also provide the following safeguards in relation to a report of the commissioner prepared under Recommendation 10-15 or 10-16 above:**

- (a) the report must not include personal information about an individual unless the individual has previously published the information, or gave the information for the purpose of publication; and
- (b) the report must not make an adverse comment about a person unless the commissioner has given the person an opportunity to respond, in writing, to the proposed comment and any response from the person is fairly stated in the report.

For paragraph (a), 'personal information' has the same meaning as under the *Information Privacy Act 2009*, section 12.

For paragraph (b), 'adverse comment' does not include a statement that a person did not participate in resolving a complaint under the legislation.

*[See Surveillance Devices Bill 2020 cll 86 and 87]*

**Protections and offences**

**10-18** The draft Bill should include the following protective provisions and offences relating to the actions of and dealings with the commissioner, to ensure the effective operation of the commissioner's functions:

- (a)** The commissioner is protected from civil liability for acts done or omissions made honestly and without negligence under the legislation.
- (b)** Where a person, acting honestly, gives information or a written response to the commissioner under a provision of the legislation:
  - (i)** the person is not liable (civilly, criminally or under an administrative process) because the person gave the information or written response; and
  - (ii)** the person cannot be held to have breached a code of professional etiquette or ethics or departed from accepted standards of professional conduct because the person gave the information or written response.
- (c)** A person who is or has been the commissioner or a staff member of the commission and who, in that capacity, acquires or has access to or custody of confidential information must not make a record of or disclose the information to another person. This does not apply if the record is made or the information is disclosed with the consent of each person to whom the record or information relates, in performing a function under the legislation, or as required or permitted under another Act. 'Confidential information' means any information that:
  - (i)** relates to a complaint made under the legislation;
  - (i)** is personal information about a complainant, respondent or another individual;
  - (iii)** is about a person's financial position or background; or
  - (iv)** if disclosed, would be likely to damage the commercial activities of a person to whom the information relates.

This does not include information that is publicly available or to statistical or other information that is not likely to identify the person to whom it relates.

- (d) A person who is or has been the commissioner, or a staff member of the commission, cannot be required to give information related to the performance of functions under the legislation to a court. This does not apply if the information is given in performing a function under the legislation, or as required or permitted by another Act.
- (e) It is an offence, with a maximum penalty of 10 penalty units:
  - (i) for a person, in the administration of the legislation, to give information to the commissioner or a staff member of the commission that the person knows is false or misleading in a material particular; or
  - (ii) for a person to fail, without reasonable excuse, to comply with a direction of the commissioner, given in a notice, requiring the person to give information to the commissioner. It is a reasonable excuse for this provision if compliance would require disclosure of information that is the subject of legal professional privilege, or information that might tend to incriminate the individual.

*[See Surveillance Devices Bill 2020 cl 76(5)–(6), 88, 89, 90, 91 and 92, sch 1 (definition of ‘information’)]*

## CHAPTER 11: GENERAL MATTERS

### Regulation-making power

- 11-1 The draft Bill should provide that the Governor in Council may make regulations under the legislation.

*[See Surveillance Devices Bill 2020 cl 94]*

### Review of Act

- 11-2 The draft Bill should provide that the Minister must complete a review of the effectiveness of the legislation within five years after the commencement. In completing the review, the Minister must consider:

- (a) whether the legislation is achieving its purpose; and
- (b) how surveillance devices and surveillance device technologies are used in civil society; and
- (c) developments in surveillance device technology; and

- (d) whether the legislation should be amended to provide for:
  - (i) new types of surveillance devices; or
  - (ii) new uses of surveillance devices and surveillance device technologies in civil society.

In addition, the Minister must table in the Legislative Assembly a report on the outcome of the review as soon as practicable after the review is completed.

*[See Surveillance Devices Bill 2020 cl 95]*

#### **Consequential provisions**

- 11-3 If legislation based on the draft Bill is enacted, the references to the '*Invasion of Privacy Act 1971*' in the following Acts should be omitted and replaced by references to the legislation, as appropriate:
- (a) the *Commissions of Inquiry Act 1950*;
  - (b) the *Fisheries Act 1994*;
  - (c) the *Police Powers and Responsibilities Act 2000*;
  - (d) the *Public Safety Preservation Act 1986*; and
  - (e) the *Youth Justice Act 1992*.



# Chapter 1

## Introduction

THE TERMS OF REFERENCE .....	1
The Consultation Paper .....	2
Submissions .....	2
The structure of this Report.....	3
TERMINOLOGY .....	4

### THE TERMS OF REFERENCE

1.1 On 24 July 2018, the Attorney-General referred to the Queensland Law Reform Commission (the ‘Commission’) ‘the issue of modernising Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies’ for review.<sup>1</sup>

1.2 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:<sup>2</sup>

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.

---

<sup>1</sup> The QDS (2018), which was released by the Queensland Government in June 2018, recommended that a number of actions be taken to promote national and international investment, increase industry and workforce capability, increase research and development, support community-friendly drone policies and improve government service delivery. The recommended actions included that the Queensland Government refer the question of ‘whether Queensland’s legislation adequately protects individuals’ privacy in the context of modern and emerging technologies’ to the Commission: QDS (2018) 31–3, 40.

<sup>2</sup> The terms of reference are set out in Appendix A.

1.3 The terms of reference exclude Queensland's existing law regulating the use of surveillance devices for State law enforcement purposes from the review.<sup>3</sup>

1.4 The terms of reference also exclude the issue of whether there should be a legislative framework to regulate the surveillance of workers by employers using surveillance devices.<sup>4</sup> This issue is the subject of a separate reference to the Commission.<sup>5</sup>

1.5 The Commission is required to report on the outcomes of the review by 28 February 2020, and to provide draft legislation based on its recommendations.<sup>6</sup>

## The Consultation Paper

1.6 In December 2018, the Commission released a Consultation Paper outlining the key issues raised in the review and calling for submissions on a number of specific questions in relation to those and other issues.

1.7 A media statement to publicise the release of the Consultation Paper and call for submissions was issued to the print and electronic media on 21 December 2018.

1.8 An advertisement calling for submissions in response to the Consultation Paper was placed in *The Weekend Australian* and *The Courier Mail* newspapers and in 12 Queensland regional newspapers on 22 December 2018, and in two other Queensland regional newspapers on 4 January 2019 and 12 January 2019.

1.9 In January 2019, notices calling for submissions were also placed on the Commission's website, on the Queensland Government 'qld.gov.au' website and 'Get Involved' website. The Queensland Law Society also published the call for submissions in the QLS Update (an electronic newsletter of the Queensland Law Society) on 23 January 2019.

1.10 The closing date for submissions was 31 January 2019.

## Submissions

1.11 The Commission received 47 written submissions from respondents, including Queensland Government departments, local governments, the OIC and

---

<sup>3</sup> See terms of reference, para E in Appendix A. See, in relation to other laws regulating surveillance devices for State law enforcement purposes, [2.40] ff below.

<sup>4</sup> See terms of reference, para F in Appendix A.

<sup>5</sup> 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/Amended-Workplace-surveillance-ToRs.pdf](https://www qlrc qld gov au/ data/assets/pdf_file/0005/589514/Amended-Workplace-surveillance-ToRs.pdf)>. The reporting date for that review is 30 April 2021.

<sup>6</sup> 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: 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. On 3 October 2019, the Attorney-General amended the terms of reference to extend the reporting date from 31 October 2019 to 28 February 2020: 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 3 October 2019.



other statutory bodies, legal profession bodies, industry representative bodies, academics and members of the public.<sup>7</sup>

1.12 The Commission was also assisted by the provision of information on matters relating to surveillance technologies and practices from organisations and individuals, including the Queensland Police Service and other Queensland Government departments, the Office of Fair Trading (Queensland), a number of approved security industry associations and the Civil Aviation Safety Authority.

1.13 The Commission wishes to thank everyone who has provided information or made a submission, or otherwise assisted with this review.<sup>8</sup>

### **The structure of this Report**

1.14 Chapter 2 provides an overview of the role of privacy and the use of surveillance devices and technologies in civil society, and the current legal framework for the regulation of surveillance devices.

1.15 Chapter 3 explains the Commission's view that there should be new legislation—in the form of the draft Bill based on the Commission's recommendations—to regulate the use, and the communication or publication of information obtained from the use, of a surveillance device.

1.16 Chapter 4 discusses the intended scope of the draft Bill and important definitions, including those for particular categories of surveillance devices covered by the draft Bill.

1.17 Chapters 5 and 6 respectively deal with the proposed criminal prohibitions on the use of a surveillance device (the 'use prohibitions'), and criminal prohibitions on the communication or publication of information obtained from the use of a surveillance device (the 'communication or publication prohibitions'). These chapters also deal with the circumstances in which a person would not commit an offence against those prohibitions, because an exception applies.

1.18 Chapter 7 deals with other matters that are ancillary to the proposed use prohibitions and the communication or publication prohibitions, as well as other issues considered in the review.

1.19 Chapter 8 deals with the proposed new civil provisions imposing general obligations not to interfere with the surveillance privacy of individuals.

1.20 Chapter 9 discusses the proposed process for complaints about contraventions of the general obligations, and civil remedies.

1.21 Chapter 10 deals with the establishment and functions of the proposed new regulator.

1.22 Chapter 11 considers general operational aspects of the draft Bill.

---

<sup>7</sup> The respondents are listed in Appendix B.

<sup>8</sup> In particular, the Commission wishes to acknowledge the valuable contribution made to the review by the late Professor Des Butler, the author of Submission 19.

- 1.23 The terms of reference are set out in Appendix A.
- 1.24 The respondents to the review are listed in Appendix B.
- 1.25 Appendix C contains comparative tables of the main provisions of the draft Bill and the surveillance devices legislation in each Australian jurisdiction.
- 1.26 Appendix D summarises other laws relevant to surveillance and privacy.
- 1.27 Appendix E summarises selected civil surveillance law reform reviews and other relevant inquiries in other jurisdictions.
- 1.28 The draft Bill, which gives effect to the Commission's recommendations, is contained in Appendix F.

## **TERMINOLOGY**

- 1.29 A list of Abbreviations and Glossary of terms commonly used in this Report is set out at the beginning of the Report

# Chapter 2

## Background

SURVEILLANCE AND SURVEILLANCE DEVICE TECHNOLOGIES.....	5
PRIVACY.....	7
SURVEILLANCE DEVICES LEGISLATION .....	9
Queensland: <i>Invasion of Privacy Act 1971</i> .....	9
Other jurisdictions .....	11
Criminal penalties.....	16
Surveillance and law enforcement in Queensland.....	17
OTHER LAWS RELEVANT TO SURVEILLANCE AND PRIVACY .....	17

### SURVEILLANCE AND SURVEILLANCE DEVICE TECHNOLOGIES

2.1 In ordinary usage, ‘surveillance’ means ‘watching over’ a person.<sup>1</sup> In the context of surveillance devices legislation, it is generally understood to involve the 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.<sup>2</sup> Further, it may be overt or covert, or a combination of both.<sup>3</sup>

2.2 Different forms of surveillance capture different types of information, for example:<sup>4</sup>

- Listening technologies, such as directional microphones, voice recorders or ‘bugs’, capture conversations or other sounds. They could also be used to intercept communications, such as phone conversations or voice communications over the internet.
- Optical technologies, such as telescopes or binoculars, can be used to monitor a person or place. Some can also be used to record or stream images, such as cameras, video recorders or CCTV.

<sup>1</sup> *Macquarie Dictionary* (online at 10 January 2020) ‘Surveillance’. See also 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; and QLRC Consultation Paper No 77 (2018) [2.21]–[2.22].

<sup>2</sup> See ALRC Report No 108 (2008) [9.89]; VLRC Report No 18 (2010) [1.11]–[1.14]; NSWLRC Report No 108 (2005) [1.8]; ACT Review (2016) [3.1].

<sup>3</sup> The distinction between overt and covert surveillance is not always clear: NSWLRC Issues Paper No 12 (1997) [2.3]. See further 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.

<sup>4</sup> See, eg, R Clarke, *A Framework for Surveillance Analysis* (Xamax Consultancy Pty Ltd, 2012) <<http://www.rogerclarke.com/DV/FSA.html>>; K Michael and R Clarke, ‘Location and Tracking of Mobile Devices: Ubervigilance Stalks the Streets’ (2013) 29(3) *Computer Law & Security Review* 216, [3]; VLRC Consultation Paper No 7 (2009) [1.13]–[1.16]; NSWLRC Issues Paper No 12 (1997) [2.3]–[2.8].

- Data surveillance technologies, such as spyware and keystroke monitors, capture data and can be used to monitor the actions or communications of an individual, including email communications or internet activities.
- Location and tracking technologies, such as GPS and radio frequency identification ('RFID'), are used to observe or record the location of an individual, vehicle or thing.

2.3 Surveillance device technologies have become increasingly sophisticated, with advanced capabilities and internet connectivity.<sup>5</sup> At the same time, they are becoming smaller, less expensive, more accessible and widely available. It is anticipated that surveillance devices will become increasingly autonomous, intelligent and connected in the future, and that the trend towards convergence will continue.<sup>6</sup>

2.4 Surveillance devices include those that are developed specifically for surveillance purposes, as well as those that are capable of being used for surveillance. A smartphone is an example of a device that is capable of being used as a surveillance device because of its camera, video and audio recording capabilities, GPS and location tracking software and internet connectivity. A drone is another example of an emerging technology capable of being used as a surveillance device, given its potential capabilities for recording images, videos and sounds.<sup>7</sup>

2.5 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, protection of personal safety and private property, marketing and research or workplace monitoring.<sup>8</sup>

2.6 It is also possible, however, for surveillance device technologies to be used for improper or harmful purposes such as theft, stalking, harassment, bullying, peeping or prying, and a range of commercial activities from espionage to covert consumer targeting.

---

<sup>5</sup> 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.

<sup>6</sup> 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; J Waldo, HS Lin and LI Millett (eds), *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press, 2007); AAUS and Liberty Victoria Paper (2015) 8–10; VLRC Consultation Paper No 7 (2009) ch 2; and QLRC Consultation Paper No 77 (2018) [2.27]–[2.36].

<sup>7</sup> QDS (2018) 9, 31.

<sup>8</sup> Workplace surveillance is excluded from this review: see terms of reference, para F in Appendix A. It is the subject of a separate reference to the Commission.

2.7 Whatever the purpose, surveillance device technologies have the potential to impact on individual privacy.<sup>9</sup> Research shows generally high levels of community concern about privacy and surveillance.<sup>10</sup>

## PRIVACY

2.8 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.<sup>11</sup>

2.9 Privacy may be described in a general way as the interest an individual has in controlling what others know about them, in being left alone and in being free from interference or intrusion.<sup>12</sup> It is often understood in terms of ‘boundaries’:<sup>13</sup>

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.

2.10 It does not depend on the classification of a physical space as ‘private’ rather than ‘public’.<sup>14</sup> Nor does it necessarily imply secrecy. Rather, privacy is the interest an individual has in controlling who has access to different aspects of their lives and when.<sup>15</sup>

2.11 There are many related and overlapping categories of privacy, including:<sup>16</sup>

- *Bodily privacy* (or ‘privacy of the person’)—the interest in restricting interference with the individual’s physical person and bodily integrity.

<sup>9</sup> See further QLRC Consultation Paper No 77 (2018) [2.37] ff.

<sup>10</sup> Ibid [2.52] ff. See also M Riedlinger, C Chapman and P Mitchell, Location awareness and geodata sharing practices of Australian smartphone users (QUT Digital Media Research Centre, September 2019); ACCC Digital Platforms Inquiry Report (2019) 382 ff, referring to Roy Morgan Research, *Consumer Views and Behaviours on Digital Platforms* (November 2018).

<sup>11</sup> 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.

See further the discussion in QLRC Consultation Paper No 77 (2018) [2.1]–[2.20].

<sup>12</sup> See, eg, International Association of Privacy Professionals (‘IAPP’), *What does privacy mean?* (2018) <<https://iapp.org/about/what-is-privacy/>>. Privacy has long been expressed as the ‘right to be let alone’: see SD Warren and LD Brandeis, ‘The Right to Privacy’ (1890) 4(5) *Harvard Law Review* 193, 195.

<sup>13</sup> Privacy International, *What is privacy?* <<https://privacyinternational.org/explainer/56/what-privacy>>. See also, eg, VLRC Occasional Paper (2002) 5; S Wong, ‘The concept, value and right of privacy’ (1996) 3 *UCL Jurisprudence Review* 165, 167–9.

<sup>14</sup> ‘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).

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

<sup>16</sup> See, eg, IAPP, *Glossary of Privacy Terms* (2018) (definitions of ‘privacy, four classes of’ and related definitions) <<https://iapp.org/resources/glossary/>>; RL Finn, M Friedewald and D Wright, ‘Seven types of privacy’ in S Gutwirth et al (eds), *European Data Protection: Coming of Age* (Springer, 2013) 3.

- *Territorial privacy* (or ‘privacy of personal space’)—the interest in limiting intrusion into personal spaces, including in the home, workplace and in public. This concerns an individual’s sense of personal safety and dignity as well as their property rights.
- *Information and data privacy*—the interest in controlling access to, use and disclosure of information about the individual, including images and information ‘derived from analysis’ of other data.<sup>17</sup>
- *Locational or tracking privacy*—the interest in controlling the extent to which information about an individual’s current or past location(s) is accessed and used by others.<sup>18</sup>
- *Behavioural privacy*—the interest in not being unduly observed or interfered with in relation to the individual’s activities, movements, associations and preferences, including sensitive matters such as sexual preferences, political activities and religious practices.<sup>19</sup>

2.12 Of central concern in the present review is the specific category of:<sup>20</sup>

- *Privacy from surveillance* (including ‘communications privacy’)—the interest in not being subject to surveillance and in not having the individual’s communications intercepted.

2.13 The ALRC observed that breaches of this category of privacy:<sup>21</sup>

may, but will not necessarily, involve breaches of territorial privacy, privacy of the person and information privacy. Communications privacy may be breached by use of listening devices, telephone taps or by mail opening. Surveillance privacy also includes, for example, surreptitious optical surveillance.

2.14 The LRC Ireland explained that privacy from surveillance:<sup>22</sup>

is based on the idea of a legal shield or boundary, the penetration of which by outside persons is prohibited except under specific circumstances laid down by law, which protects the individual from privacy-invasive surveillance ... in all of the spheres recognised [as privacy interests]. Moreover, an unlawful crossing of that boundary ([for example] by placing an electronic device in a person’s home, by tapping his telephone or by systematically spying on his movements even in public places) may occur even though no private or intimate information is in fact obtained as a result.

<sup>17</sup> See Waldo, Lin and Millett (eds), above n 6, 22.

<sup>18</sup> See, eg, K Michael and R Clarke, ‘Location and Tracking of Mobile Devices: Ueberveillance Stalks the Streets’ (2013) 29(3) *Computer Law & Security Review* 216, [5.1].

<sup>19</sup> See, eg, R Clarke, ‘The regulation of civilian drones’ impacts on behavioural privacy’ (2014) 30(3) *Computer Law & Security Review* 286, [2.2].

<sup>20</sup> See, eg, ALRC Report No 22 (1983) [46]; LRC Ireland Report No 57 (1998) [2.4], [2.10]. The LRC Ireland referred to this as ‘freedom from privacy-invasive surveillance’.

<sup>21</sup> ALRC Report No 22 (1983) [46].

<sup>22</sup> LRC Ireland Report No 57 (1998) [2.5].

2.15 As with other aspects of privacy, the extent of an individual's interest in not being subject to surveillance will depend on the particular circumstances, including whether the individual has a 'reasonable expectation' of privacy.<sup>23</sup>

2.16 Privacy is recognised as a fundamental value of importance to individual autonomy and dignity, and as a core element of modern liberal democracy.<sup>24</sup>

2.17 It 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 Act 2019* and in the human rights statutes of some other jurisdictions.<sup>25</sup>

2.18 Privacy is not absolute.<sup>26</sup> It must be balanced against other countervailing rights and interests. This includes freedom of expression and opinion which, like privacy, is recognised as a human right.<sup>27</sup>

## SURVEILLANCE DEVICES LEGISLATION

2.19 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').<sup>28</sup>

### Queensland: *Invasion of Privacy Act 1971*

2.20 In Queensland, the *Invasion of Privacy Act 1971* regulates listening devices. Section 4 of the Act defines a 'listening device' as:<sup>29</sup>

<sup>23</sup> ALRC Report No 22 (1983) [1186]; LRC Ireland Report No 57 (1998) [2.10]; ALRC Report No 123 (2014) [6.5].

<sup>24</sup> See, eg, JL Mills, *Privacy: The Lost Right* (Oxford University Press, 2008) 26–7; ALRC Report No 123 (2014) [2.6]; VLRC Occasional Paper (2002) 17–20, 22; and 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. Privacy can be conceived as a public and collective value: see, eg, ALRC Report No 123 (2014) [2.16] ff.

The AHRC has proposed that the Australian Government develop a national strategy for the protection of human rights, including the right to privacy, in the design, development and use of new and emerging technologies: AHRC Discussion Paper (2019) 39–41, Proposal 1. A final report is due in 2020.

<sup>25</sup> See the discussion of the *Human Rights Act 2019* (Qld) at [D.15]–[D.17] below.

<sup>26</sup> See generally Waldo, Lin and Millett (eds), above n 6, 22–5.

Some interests are complementary to privacy, such as confidentiality, reputation and non-discrimination. Others potentially conflict with privacy, including freedom of expression, the promotion of open justice, national security, the prevention and detection of crime and fraud, and freedom from violence: see ALRC Report No 22 (1983) [68]–[74]; and ALRC Report No 123 (2014) [2.22].

<sup>27</sup> In the context of arts 17, 19(2) of the ICCPR, see QLRC Consultation Paper No 77 (2018) App E. On the other hand, privacy can also enhance freedom of expression and innovation: JE Cohen, 'What Privacy is For' (2013) 126(7) *Harvard Law Review* 1904, 1905–06. See also, eg, NSWLRC Report No 108 (2005) [3.28].

<sup>28</sup> See Table 1 in Appendix C below.

<sup>29</sup> However, s 42(1) of the *Invasion of Privacy Act 1971* (Qld) provides that a reference to a 'listening device':

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.

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.

2.21 The use of a listening device is regulated only to the extent that it is used in relation to a private conversation. Section 4 of the Act defines a ‘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.

2.22 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’).<sup>30</sup> Use by a party without the consent of the other parties—referred to as ‘participant monitoring’—is therefore permitted.<sup>31</sup>

2.23 A reference to a ‘party’ is a reference:<sup>32</sup>

- (a) to a person by or to whom words are spoken in the course of a private conversation; and
- (b) to 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.

2.24 There are also prohibitions on communicating or publishing information (the ‘communication or publication prohibitions’). In particular:

- a party to a private conversation 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;<sup>33</sup> 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.<sup>34</sup>

<sup>30</sup> *Invasion of Privacy Act 1971* (Qld) s 43(1), (2)(a). 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).

<sup>31</sup> See also [2.36] below.

<sup>32</sup> *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 [2.34]–[2.35] below. Each of those terms is used where relevant in this Report.

<sup>33</sup> *Invasion of Privacy Act 1971* (Qld) s 45(1). A party is also prohibited from communicating a statement prepared from a record of the conversation.

<sup>34</sup> *Invasion of Privacy Act 1971* (Qld) s 44(1).



2.25 There are exceptions to each of these prohibitions, including if the communication or publication is made with the consent of a party to the conversation.<sup>35</sup>

2.26 The *Invasion of Privacy Act 1971* also contains ancillary prohibitions, including that:<sup>36</sup>

- where a private conversation has come to a person's knowledge as the direct or indirect result of the unlawful use of a listening device, it is an offence to give evidence of the conversation in civil or criminal proceedings, unless an exception applies;<sup>37</sup> and
- it is an offence to advertise a listening device of a prescribed class or description.<sup>38</sup>

## Other jurisdictions

2.27 Like Queensland, the surveillance devices legislation in the Australian Capital Territory and Tasmania regulates the use of listening devices in relation to private conversations.<sup>39</sup>

2.28 In contrast, the surveillance devices legislation in New South Wales, the Northern Territory, South Australia, Victoria and Western Australia extends to additional categories of surveillance devices.<sup>40</sup>

2.29 In those jurisdictions, a 'surveillance device' is defined to mean a listening device, an optical surveillance device, a tracking device or, except in Western Australia, a data surveillance device.<sup>41</sup> A 'listening device' is defined in similar terms

---

<sup>35</sup> See *Invasion of Privacy Act 1971* (Qld) ss 44(2), 45(2).

<sup>36</sup> See also, in relation to unlawful entry of a dwelling, *Invasion of Privacy Act 1971* (Qld) s 48A, which is discussed at [7.47] ff below.

<sup>37</sup> *Invasion of Privacy Act 1971* (Qld) s 46, which is discussed at [7.64] ff below.

<sup>38</sup> *Invasion of Privacy Act 1971* (Qld) s 48, which is discussed at [7.9] ff below. No devices have been prescribed.

<sup>39</sup> *Listening Devices Act 1992* (ACT); *Listening Devices Act 1991* (Tas).

<sup>40</sup> 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); 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).

<sup>41</sup> *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).

to the legislation in Queensland.<sup>42</sup> The other categories of surveillance devices are defined as follows:<sup>43</sup>

- *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 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).<sup>44</sup> This does not include an optical surveillance device. In South Australia, it is also defined as a device that can access or track the input or output of that information and associated equipment.<sup>45</sup>

2.30 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.<sup>46</sup>

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

<sup>42</sup> See [2.20] 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 43 below.

<sup>43</sup> *Surveillance Devices Act 2007* (NSW) s 4(1) (definitions of ‘computer’, ‘device’, ‘listening device’, ‘optical surveillance device’, ‘tracking device’ and ‘data surveillance device’); *Surveillance Devices Act* (NT) s 4 (definitions of ‘computer’, ‘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 ‘computer’, ‘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’).

<sup>44</sup> 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.

<sup>45</sup> ‘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) (definition of ‘associated equipment’).

<sup>46</sup> See n 41 above. No other kind of device has been prescribed by regulation in those jurisdictions.

- 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).<sup>47</sup>
- An *optical surveillance device* is regulated:
  - only in relation to a 'private activity' (except in New South Wales);<sup>48</sup>
  - 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 onto or into the premises or vehicle, or interference with the vehicle or other object, without consent.<sup>49</sup>
- 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.<sup>50</sup>
- A *data surveillance device* is regulated:
  - in the Northern Territory and Victoria, only in relation to law enforcement officers;<sup>51</sup>
  - 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;<sup>52</sup>
  - 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.<sup>53</sup>

<sup>47</sup> *Listening Devices Act 1992* (ACT) s 4(1); *Surveillance Devices Act 2007* (NSW) s 7(1); *Surveillance Devices Act* (NT) s 11(1); *Surveillance Devices Act 2016* (SA) s 4(1); *Listening Devices Act 1991* (Tas) s 5(1); *Surveillance Devices Act 1999* (Vic) s 6(1); *Surveillance Devices Act 1998* (WA) s 5(1).

<sup>48</sup> *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 56 below.

<sup>49</sup> See *Surveillance Devices Act 2007* (NSW) ss 4(1) (definition of 'premises'), 8(1); *Surveillance Devices Act 2016* (SA) ss 3(1) (definition of 'premises'), 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.

<sup>50</sup> *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.

<sup>51</sup> *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9. In the Northern Territory, the legislation also regulates the use of a data surveillance device by an ICAC officer.

<sup>52</sup> *Surveillance Devices Act 2007* (NSW) s 10(1). For the meaning of 'premises', see n 49 above.

<sup>53</sup> *Surveillance Devices Act 2016* (SA) s 8(1).

### **Definitions of ‘private conversation’, ‘private activity’ and ‘party’**

2.32 The regulation of a listening device is linked to the concept of a ‘private conversation’ and, except in New South Wales, the regulation of an optical surveillance device is linked to the concept of a ‘private activity’. Consistently with the legislation in Queensland,<sup>54</sup> these concepts are defined as follows:<sup>55</sup>

- *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.<sup>56</sup>

2.33 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.<sup>57</sup>

2.34 A ‘party’ to a private conversation is defined:<sup>58</sup>

---

<sup>54</sup> See [2.21] above.

<sup>55</sup> *Listening Devices Act 1992* (ACT) s 2 Dictionary (definition of ‘private conversation’); *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of ‘private conversation’); *Surveillance Devices Act* (NT) s 4 (definitions of ‘private conversation’ and ‘private activity’); *Surveillance Devices Act 2016* (SA) s 3(1) (definitions of ‘private conversation’ and ‘private activity’); *Listening Devices Act 1991* (Tas) s 3(1) (definition of ‘private conversation’); *Surveillance Devices Act 1999* (Vic) s 3(1) (definitions of ‘private conversation’ and ‘private activity’); *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of ‘private conversation’ and ‘private activity’).

<sup>56</sup> 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 49 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].

<sup>57</sup> See also ACT Review (2016) [6.7], in which it was recommended the 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:

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.

<sup>58</sup> *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’).

- 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.

2.35 In the Northern Territory and Victoria, a 'party' to a private activity is defined as a person who takes part in the activity.<sup>59</sup> However, in Western Australia a person who takes part in the activity is a 'principal party', and a 'party' is a person who takes part in the activity or observes or records the activity with the express or implied consent of a principal party.<sup>60</sup>

### **Participant monitoring**

2.36 In the Northern Territory and Victoria (like 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 party or parties.<sup>61</sup> 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.<sup>62</sup>

### **Communication or publication prohibitions**

2.37 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 to a private conversation and to another person.<sup>63</sup> Other jurisdictions include more general offence provisions that apply to any user of a relevant surveillance device.<sup>64</sup> The provisions vary in their application to information that was obtained through the lawful or unlawful use of a device.

<sup>59</sup> *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'.

<sup>60</sup> *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of 'party' and 'principal party').

<sup>61</sup> *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 the persons being recorded, may also have a similar effect: *Surveillance Devices Act 2007* (NSW) s 8(1).

<sup>62</sup> *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 61 above.

<sup>63</sup> *Listening Devices Act 1992* (ACT) ss 5, 6; *Listening Devices Act 1991* (Tas) ss 9, 10. For a discussion of the Queensland provisions, see [2.24]–[2.25] above.

<sup>64</sup> *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.

## Exceptions

2.38 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 includes use, communication or publication with the consent of the parties to the private conversation or activity.

## Criminal penalties

2.39 The maximum penalties for the primary offences under surveillance devices legislation are as follows:<sup>65</sup>

	Maximum penalty for an individual		Maximum penalty for a corporation
	Use prohibitions	Communication or publication prohibitions	
<b>Qld</b>	40 penalty units (\$5338) or 2 years imprisonment	40 penalty units (\$5338) or 2 years imprisonment	200 penalty units (\$26 690)
<b>ACT</b>	50 penalty units (\$8000)	50 penalty units (\$8000) or 6 months imprisonment or both	50 penalty units (\$40 500)
<b>NSW</b>	100 penalty units (\$11 000) or 5 years imprisonment or both	100 penalty units (\$11 000) or 5 years imprisonment or both	500 penalty units (\$55 000)
<b>NT</b>	250 penalty units (\$39 250) or 2 years imprisonment	250 penalty units (\$39 250) or 2 years imprisonment	1250 penalty units (\$196 250)
<b>SA</b>	\$15 000 or 3 years imprisonment	\$15 000 or 3 years imprisonment (where device used in contravention of the Act) or \$10 000 (in other specified cases)	\$75 000 (where device used in contravention of the Act) or \$50 000 (in other specified cases)
<b>Tas</b>	40 penalty units (\$6720) or 2 years imprisonment or both	40 penalty units (\$6720) or 2 years imprisonment or both	500 penalty units (\$84 000)
<b>Vic</b>	240 penalty units (\$39 652.80) or 2 years imprisonment or both	240 penalty units (\$39 652.80) or 2 years imprisonment or both	1200 penalty units (\$198 264)
<b>WA</b>	\$5000 or 12 months imprisonment or both	\$5000 or 12 months imprisonment or both	\$50 000

<sup>65</sup> 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 \$157); *Surveillance Devices Act 2016* (SA) ss 4(1), 5(1)–(3), 7(1), 8(1), 9(1)–(3), 10(1), 12(1); *Invasion of Privacy Act 1971* (Qld) ss 43(1), 44(1), 45(1) and *Penalties and Sentences Regulation 2015* (Qld) s 3 (value of penalty unit \$133.45); *Listening Devices Act 1991* (Tas) s 12 and Tasmania, *Government Gazette* No 21885, 22 May 2019, 308 (value of penalty unit \$168); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1), 11(1) and Victoria, *Government Gazette* No G14, 4 April 2019, 572 (value of penalty unit \$165.22); *Surveillance Devices Act 1998* (WA) ss 5(1), 6(1), 7(1), 9(1).

The *Invasion of Privacy Act 1971* (Qld) 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 s 181B of the *Penalties and Sentences Act 1992*. Provision to similar effect applies in the Northern Territory under the *Interpretation Act* (NT) s 38DB.

## Surveillance and law enforcement in Queensland

2.40 In Queensland, chapter 13 of the PPRA separately regulates the use of a listening device, an optical surveillance device, a tracking device or a data surveillance device by law enforcement officers.<sup>66</sup> The *Surveillance Devices Act 2004* (Cth) regulates the use of those devices by federal law enforcement officers.

2.41 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 the use of a surveillance device. The PPRA provides for the recognition of warrants and authorisations issued in other Australian jurisdictions.<sup>67</sup>

2.42 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.<sup>68</sup> The model legislation was deliberately similar to existing state and territory legislation because the intention was to achieve harmonisation and facilitate cross-border operations.<sup>69</sup>

2.43 The model legislation was implemented in Queensland by the insertion of chapter 13 of the PPRA.<sup>70</sup> 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.<sup>71</sup>

## OTHER LAWS RELEVANT TO SURVEILLANCE AND PRIVACY

2.44 In Queensland, surveillance and privacy are also regulated by other State and Commonwealth legislation. As well, there are a few common law causes of action that may be relevant in the context of civil surveillance. Some key aspects of those laws are discussed in Appendix D below.

---

<sup>66</sup> See also the *Crime and Corruption Act 2001* (Qld) ch 3 pt 6, which regulates the use of a surveillance device by authorised officers of the Crime and Corruption Commission. That 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 in Appendix A.

<sup>67</sup> See generally *Police Powers and Responsibilities Act 2005* (Qld) s 321; *Surveillance Devices Act 2004* (Cth) s 3.

<sup>68</sup> 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.

<sup>69</sup> Joint Working Group Report (2003) 347.

<sup>70</sup> See *Cross-Border Law Enforcement Legislation Amendment Act 2005* (Qld) s 28.

<sup>71</sup> See, eg, *Surveillance Devices Act 2007* (NSW); Explanatory Note, Surveillance Devices Bill 2007 (NSW) 1. See also Explanatory Note, Surveillance Devices Amendment (Statutory Review) Bill 2018 (NSW) 1.





## Chapter 3

# A new approach to regulating the use of surveillance devices

INTRODUCTION .....	19
The need for new surveillance devices legislation in Queensland .....	20
THE COMMISSION'S APPROACH .....	21
Balancing surveillance and privacy .....	21
Consent .....	22
Exceptions for authorised use .....	22
Exceptions for justified and 'reasonably necessary' purposes .....	23
A criminal law and a civil law response .....	23
The draft Bill .....	23
ALTERNATIVE APPROACHES .....	24
RECOMMENDATION .....	28

### INTRODUCTION

3.1 In Queensland, the *Invasion of Privacy Act 1971* regulates the use of listening devices; however, it does not apply to other categories of surveillance devices.

3.2 In most other Australian jurisdictions, surveillance devices legislation has been modernised and updated to regulate not only the use of listening devices, but also the use of optical surveillance devices, tracking devices and, in some jurisdictions, data surveillance devices.<sup>1</sup> This broader scope protects a greater range of activities and information about which an individual may have a reasonable expectation of privacy.

3.3 All existing surveillance devices legislation regulates the use of surveillance devices through criminal prohibitions only; it does not provide a civil complaints mechanism or civil remedy provisions.

3.4 Other laws offer only limited protection for the privacy of individuals in relation to the use of surveillance devices.

---

<sup>1</sup> The surveillance devices legislation in the Australian Capital Territory and Tasmania regulates the use of listening devices only. 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 QLRC Consultation Paper No 77 (2018) [D.23] ff.

3.5 The IP Act and the Privacy Act each apply in limited circumstances and do not generally protect the privacy of individuals against surveillance.<sup>2</sup> In particular, the Acts collectively:<sup>3</sup>

- apply only to the collection and use of ‘personal information’;<sup>4</sup>
- apply to government agencies and a limited class of other entities;<sup>5</sup> and
- do not apply to all businesses, or to individuals acting in a private capacity.<sup>6</sup>

3.6 Criminal offences relating to the use of surveillance devices or information obtained from such use operate to protect the privacy of an individual, but they do not confer any right upon the individual to bring a civil proceeding or obtain redress.

3.7 Whilst there are some civil causes of action that may indirectly protect an individual’s privacy in relation to the use of surveillance devices, such as trespass, nuisance or breach of confidence, they are not intended specifically to deal with breaches of privacy and provide ‘only ... piecemeal, limited protection’.<sup>7</sup>

### The need for new surveillance devices legislation in Queensland

3.8 In the Commission’s view, there are gaps and uncertainties in the current laws in Queensland regulating the use of surveillance devices.

3.9 In light of the limitations of the *Invasion of Privacy Act 1971*, a more comprehensive legislative response to the use of surveillance devices is required. This response should address the range of devices and activities that should be regulated; the range of information that should be protected; and the rights of, and remedies available to, individuals whose privacy should be protected.

3.10 Accordingly, the Commission recommends the repeal of the *Invasion of Privacy Act 1971* and proposes the introduction of new legislation to protect the

<sup>2</sup> The ACCC has recommended that the reform of the *Privacy Act 1988* (Cth) to address gaps in the regulatory framework, and to extend it to apply to user data collected by digital platforms: ACCC Digital Platforms Inquiry Report (2019) Rec 16, 456ff. The Government has committed to introduce draft legislation to amend the Privacy Act, including to introduce a binding privacy code of practice that will apply to digital platforms that trade in personal information and committed to undertake a broader review of the Privacy Act: Australian Government, ‘Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry’ (2019). See further [4.73] below.

<sup>3</sup> Cf the *EU General Data Protection Regulation* which applies more broadly to data protection.

<sup>4</sup> 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].

<sup>5</sup> See, eg, D Handel, ‘The clouds have eyes—protecting privacy in the drone age’ (2017) 14(4) *Privacy Law Bulletin* 63–4.

<sup>6</sup> See, eg, Eyes in the Sky Report (2014) [4.10]–[4.11]; Hutchens and Perier, above n 4, 11; 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; Handel, above n 5, 63–4; S Hinchcliffe, ‘Drones—a “serious” invasion of privacy in the digital era?’ (2014) 11(9) *Privacy Law Bulletin* 155, 156.

<sup>7</sup> Allgrove and Grimwood-Taylor, above n 4, 35. See also, eg, Handel, above n 5, 64–5. See also QLRC Consultation Paper (2018) No 77 [2.133] ff.

privacy of individuals in relation to the use, and the communication or publication of information obtained from the use, of surveillance devices in civil society. The Commission's recommendations are given effect by the draft Bill in Appendix F below.

## THE COMMISSION'S APPROACH

3.11 The Commission's approach is informed by a number of principles and considerations, including:

- the importance of community expectations;
- the need to balance the protection of privacy and the justified use of surveillance devices;<sup>8</sup>
- the importance of consent;<sup>9</sup>
- that objective standards should form the basis for the justified use of surveillance devices in the absence of consent;<sup>10</sup>
- that the regulation of surveillance devices should be practical, and should include both a criminal law and a civil law response;<sup>11</sup>
- the desirability of reasonable consistency with surveillance devices legislation in other Australian jurisdictions;
- that surveillance devices legislation may overlap with but has a different focus from legislation that regulates information privacy and data protection;<sup>12</sup> and
- that the draft Bill should not affect the operation of other laws regulating the use of surveillance devices.<sup>13</sup>

## Balancing surveillance and privacy

3.12 The Commission takes as its starting point the need to appropriately protect an individual's privacy in relation to the use, and the communication or publication of information obtained from the use, of a surveillance device.<sup>14</sup> The extent of that privacy will depend on the particular circumstances.<sup>15</sup>

---

<sup>8</sup> See further [3.12]–[3.17] below.

<sup>9</sup> See further [3.18]–[3.19] below.

<sup>10</sup> See further [3.20]–[3.22] below.

<sup>11</sup> See further [3.23]–[3.25] below.

<sup>12</sup> See further, eg, [3.43] below.

<sup>13</sup> Some laws are expressly excluded from consideration by the terms of reference: see [1.3]–[1.4] above.

<sup>14</sup> See the terms of reference, paras 1–2 in Appendix A.

<sup>15</sup> See [2.15] above.

3.13 Further, the draft Bill should also be compatible with the *Human Rights Act 2019* and relevant human rights instruments which recognise that a person's privacy must be respected.

3.14 However, the right to privacy in relation to the use of surveillance devices must be balanced against other countervailing rights and interests. In civil society, there can be many reasons for the use of surveillance devices or for the communication or publication of information obtained from such use.

3.15 The draft Bill should focus on the individual whose privacy interests are relevant, coupled with objective standards of responsible use, communication or publication that are flexible enough to respond to the circumstances of each case.

3.16 The criminal prohibitions in the draft Bill should apply to matters that are private, including private conversations and private activities;<sup>16</sup> and information about the geographical location of a person, vehicle or thing, or information that is input into, output from, or stored in a computer.<sup>17</sup>

3.17 The civil provisions in the draft Bill should apply where the individual has a 'reasonable expectation of surveillance privacy'.<sup>18</sup> This is a question of fact, and will depend on a range of factors.

## Consent

3.18 Consent is a central authorising concept in information privacy law,<sup>19</sup> as well as under existing surveillance devices legislation. It is the appropriate concept because it confers choice on the individual as to the extent of their privacy protection.<sup>20</sup>

3.19 If there is consent, the use, communication or publication should be lawful. In the absence of consent, the use, communication or publication should be unlawful unless an exception applies.

## Exceptions for authorised use

3.20 The use of a surveillance device without consent should not be unlawful under the draft Bill if it is authorised under another Act.<sup>21</sup>

---

16 See the discussion of the meaning of 'private conversation' and 'private activity' at [5.158] ff below.

17 See the discussion of tracking devices and data surveillance devices at [5.191] ff below.

18 See the discussion at [8.61]–[8.80] below.

19 See, eg, *Information Privacy Act 2009* (Qld) sch 3 IPP 10(1)(a), 11(1)(b); *Privacy Act 1988* (Cth) sch 1 APP 3.3(a), APP 6.1(a). Consent is also a key principle of the *EU General Data Protection Regulation*: see art 6(1)(a).

20 See [2.9]–[2.10] above.

21 See further [4.7] below.

## Exceptions for justified and ‘reasonably necessary’ purposes

3.21 The scope of other exceptions under the draft Bill should be limited, where relevant, by a ‘reasonableness’ test. In general terms, the use of a surveillance device without consent should be permitted only where there is a justified purpose and, if relevant, where the use, communication or publication is ‘reasonably necessary’ for that purpose.<sup>22</sup>

3.22 A ‘reasonably necessary’ test ensures that more is required than simply identifying a relevant purpose, such as the public interest or a lawful interest, or that the use is convenient or desirable for that purpose. A surveillance device should be used only to the extent that is least restrictive of the individual’s privacy.

## A criminal law and a civil law response

3.23 The Commission considers that the draft Bill requires both a criminal and a civil component.

3.24 A criminal law response is required where the seriousness of a person’s conduct in using a surveillance device justifies the intervention of the State in imposing criminal sanctions. This approach recognises the public interest in responding to serious breaches of privacy from the unlawful use of surveillance devices.

3.25 A civil law response is required to promote the responsible use of surveillance devices in everyday contexts and to empower individuals whose privacy is affected to seek civil redress in appropriate circumstances. This approach focuses on the affected individuals who have the greatest interest in redressing breaches of their surveillance privacy.

## The draft Bill

3.26 The main purpose of the draft Bill is to provide for an individual’s privacy to be protected from unjustified interference from the use, or the communication or publication of information obtained from the use, of surveillance devices.<sup>23</sup>

3.27 To achieve this purpose, the draft Bill:

- applies to a wider range of surveillance devices than the existing legislation—in addition to applying to listening devices, it also applies to optical surveillance devices, tracking devices and data surveillance devices;
- regulates the use of surveillance devices, and the communication or publication of information obtained from such use, through criminal prohibitions;
- imposes civil law obligations not to use a surveillance device, or to communicate or publish information obtained from such use, if that would

---

<sup>22</sup> Unless, for example, the use, communication or publication is expressly authorised by another Act (in which case the requirements of the authorising Act should apply, rather than an additional ‘reasonably necessary’ requirement).

<sup>23</sup> See cl 2 of the draft Bill in Appendix F.

interfere with an individual's surveillance privacy (that is, where the individual has a reasonable expectation of surveillance privacy and has not consented to the use, communication or publication);

- provides for complaints about contraventions of those obligations to be made and resolved by mediation or, if unresolved, heard and decided by QCAT; and
- establishes an independent regulator—the Surveillance Devices Commissioner—to carry out the functions of complaints handling, research, advice and monitoring, compliance monitoring and the provision of guidance (including, promoting understanding of and compliance with the new obligations and the operation of the legislation).

## ALTERNATIVE APPROACHES

3.28 The Commission considered other possible approaches but, for the reasons discussed in this Report, prefers the approach taken in the draft Bill.<sup>24</sup>

### *Public-private distinction*

3.29 One alternative approach to regulation is to distinguish between the use of surveillance devices in public and private places. This was the approach taken by the VLRC, which was required by its terms of reference to consider legislative reforms for the appropriate control of surveillance in public places.<sup>25</sup>

3.30 Such an approach is based on the idea that different expectations of privacy may arise in public places and that, accordingly, surveillance in public places should be regulated differently.<sup>26</sup>

3.31 However, this is a matter of degree. Depending on the circumstances, a person may have a reasonable expectation of surveillance privacy in a public place.<sup>27</sup> It may be reasonable, for example, to expect privacy from surveillance when using a public bathroom or in relation to particular conversations in a secluded public area, but not in relation to other activities in a shopping centre or crowded public mall.<sup>28</sup>

---

<sup>24</sup> See especially [3.44]–[3.47] below.

<sup>25</sup> See VLRC Report No 18 (2010) [1.2]; and [E.11] ff below.

<sup>26</sup> See, eg, ALRC Report No 22 (1983) [1186], in which the ALRC recommended that there should be no regulation of optical surveillance in public places, observing that:

It is not desirable, nor would it be feasible, to regulate the use of surveillance or recording by means of optical devices in streets, parks and other such entirely public places. ... People who are in a public place must anticipate that they may be seen, and perhaps recorded, and must modify their behaviour accordingly. That is the essence of a 'public' place.

<sup>27</sup> See also [8.78], [8.80] below.

<sup>28</sup> See, eg, the discussion in D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29(2) *Melbourne University Law Review* 339, 370.

3.32 Different definitions of what is a ‘public place’ apply for different purposes.<sup>29</sup> A public-private distinction is not a clear or an easy one to draw in the context of privacy.<sup>30</sup> As Gleeson CJ explained in *ABC v Lenah Game Meats Pty Ltd*:<sup>31</sup>

There is no bright line which can be drawn between what is private and what is not. Use of the term ‘public’ is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford.

3.33 The regulation of surveillance devices on the basis of a public-private distinction oversimplifies the context. An individual’s location may be one of several relevant factors, but should not form the primary basis for regulation.<sup>32</sup>

### **Overt-covert distinction**

3.34 Another alternative approach is to distinguish between the overt and covert use of surveillance devices. This was the approach recommended by the NSWLRC in its review of surveillance devices legislation.<sup>33</sup>

3.35 This is based on the idea that covert surveillance is a more significant interference with privacy than overt surveillance and should accordingly be subject to different regulatory controls.<sup>34</sup> It has been suggested, for example, that covert surveillance is more likely to target particular individuals or groups, to capture unguarded or intimate conversations and activities, and to use more sophisticated technology.<sup>35</sup>

3.36 However, this does not reflect the capacity for overt surveillance to interfere with privacy. What distinguishes covert from overt surveillance is not the subject of the surveillance, its intrusiveness or even the sophistication of the technology

<sup>29</sup> Cf the definitions of ‘public place’ in, for example, the *Environmental Protection Act 1994* (Qld) s 7 sch 4; *Personal Injuries Proceedings Act 2002* (Qld) s 63; *Liquor Act 1992* (Qld) s 11; *Peaceful Assembly Act 1992* (Qld) s 4; *Police Powers and Responsibilities Act 2000* (Qld) sch 6; and *Summary Offences Act 2005* (Qld) s 3 sch 2.

<sup>30</sup> See, eg, NSWLRC Interim Report No 98 (2001) [2.22]–[2.23]; and [E.2] ff below.

<sup>31</sup> (2001) 208 CLR 199, [42].

<sup>32</sup> See also NSWLRC Interim Report No 98 (2001) [2.26], in which the NSWLRC observed that an approach based on a public-private distinction:

is based on the flawed assumption that a person’s legitimate expectation of privacy and freedom from surveillance depends on where they happen to be at any given time. Privacy is a personal, not a property interest, and should not diminish because a person is in a public place. (note omitted)

<sup>33</sup> See NSWLRC Interim Report No 98 (2001) [2.77]–[2.79], [2.88], Recs 9, 10, 13.

<sup>34</sup> A separate authorisation process for covert surveillance might be required, such as an application to a court for a warrant. Under existing surveillance devices legislation, this is typically reserved for law enforcement officers.

<sup>35</sup> NSWLRC Interim Report No 98 (2001) [3.29]. The NSWLRC recommended that overt surveillance should be regulated by legislative principles with a civil complaints scheme, and that covert surveillance should ordinarily require authorisation from a court or tribunal.

employed—as may be evident from the capabilities of home security cameras which may be used overtly—but the mere fact of whether notice of the surveillance is given.

3.37 However, notice does not necessarily equate with consent. Notice might be given generally, to a wide audience, or to a specific individual or group. Even with clear prior notice, there may be little opportunity for an individual to avoid becoming the subject of the surveillance. Nor does the provision of notice itself indicate whether the purpose of the use in the particular circumstances is justified.

3.38 In the Commission’s view, notice alone should not determine whether the use is lawful. Such an approach would undermine the role of consent and the importance of purpose. As explained above, in circumstances where the draft Bill applies and it is impracticable to obtain consent (for example, in the case of mass surveillance), the use of a surveillance device should be permitted only if it is for a justified purpose (that is, where it falls within one of the exceptions).

### ***Data protection approach***

3.39 A different approach is to regulate the use of data collected from surveillance devices, but not the use of the devices themselves. This approach would focus only on data protection.

3.40 This is based on the idea that the ubiquity of surveillance technology makes it impractical to regulate the use of surveillance devices. QGCIO submitted, for example, that:

the regulation of surveillance devices in this modern digital world may prove challenging, as any electronic device that collects data can be used as a surveillance device, and ... there will continue to be new devices emerging that collect an ever-expanding scope of personal and sensitive data.

...

It is on this basis that QGCIO suggests that the scope of the new legislative framework avoid regulating for specific surveillance devices, or even specific categories of surveillance devices. Rather, the new legislative framework should look to regulate any data collected or recorded by an electronic device which is subsequently used (or re-used) for surveillance purposes.

3.41 However, a data protection approach would fail to protect against the interference with privacy from the use of surveillance devices. As the NSWLRC observed, ‘[t]he threshold problem with surveillance remains the act itself: being watched or otherwise monitored. The potential intrusion on personal privacy through the use of surveillance devices ... is the most immediate concern with surveillance usage’.<sup>36</sup>

3.42 Further, a data protection approach does not take into account the fact that the use of a surveillance device will not always result in the collection of ‘data’. For example, a listening device might be used to listen to a private conversation without making a recording or otherwise collecting data. Protection from privacy-invasive

---

<sup>36</sup> NSWLRC Interim Report No 98 (2001) [3.29].



surveillance should not depend on whether or not data is collected from the use of the surveillance device.

3.43 Neither does all data collection relate to surveillance. Data protection and information privacy raise wider and substantively different issues from the use of surveillance devices. Data protection overlaps with privacy as well as with competition law and consumer protection. This includes issues such as big data, the use of artificial intelligence ('AI') in data analytics and the business practices of digital platforms.<sup>37</sup> Whilst it might be expected that progress toward a more comprehensive, coordinated (and national) privacy and data protection framework might be made in the future,<sup>38</sup> this is not presently the case.<sup>39</sup> These issues fall outside the scope of the Commission's review.

### ***The Commission's view***

3.44 The Commission's view is that each of the alternative approaches outlined above is unsatisfactory. They oversimplify the subject matter without taking account of other relevant contextual factors. This is likely to have unintended consequences with arbitrary results.

3.45 The public-private distinction and the overt-covert distinction over-emphasise where and how a surveillance device is used at the expense of other relevant factors such as the subject matter and purpose of the surveillance (as well as the role of consent).

3.46 The data protection approach discounts the incursion into privacy that occurs from the use of a surveillance device itself, focusing instead only on the subsequent use of any 'data' collected from such a device. This is a selective and limited form of protection.

3.47 The Commission's approach instead applies generally and focuses primarily on purpose. In the absence of consent, the question is whether the use, communication or publication is for a justified purpose (and whether it is reasonably necessary for that purpose).<sup>40</sup> It also continues to regulate both the use of a surveillance device and the communication or publication of information obtained from that use.

---

<sup>37</sup> See, eg, ACCC Digital Platforms Final Report (2019) 5. See also [4.73] below. See also AHRC Discussion Paper (2019) pts B and C.

<sup>38</sup> See, eg, *EU General Data Protection Regulation*.

<sup>39</sup> At the federal level, a more comprehensive data protection framework is still in progress: see, in relation to reforms to the *Privacy Act 1988* (Cth) and the sharing of public and private sector data, respectively: ACCC Digital Platforms Inquiry Report (2019), Australian Government, 'Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry' (2019); and Australian Government, *Data Availability and Use*, Productivity Commission Inquiry Report: Overview and Recommendations No 82 (31 March 2017); Department of the Prime Minister and Cabinet, The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry (2018). See also, in relation to big data guidelines, Australian Government, *Australian Public Service Better Practice Guide for Big Data* (Version 2.0, January 2015). In addition, the AHRC has proposed the introduction of a national strategy for the protection of human rights in the development and use of new and emerging technologies, including AI informed decision-making. Among other things, it has proposed the establishment of an AI Safety Commissioner: AHRC Discussion Paper (2019) pts B and C.

<sup>40</sup> There are also some additional exceptions for other authorised activities.

**RECOMMENDATION**

- 3-1    The *Invasion of Privacy Act 1971* should be repealed, and replaced by new legislation which implements the Commission's recommendations in the form of the draft Bill.**

*[See Surveillance Devices Bill 2020 cl 96 and [3.10] above]*

# Chapter 4

## Preliminary matters

THE APPLICATION OF THE DRAFT BILL .....	29
The application of the draft Bill to all persons .....	29
Relationship with other laws .....	29
THE DEFINITION OF SURVEILLANCE DEVICE AND RELATED DEFINITIONS .....	32
Approaches to the definition of surveillance device .....	32
Submissions .....	34
The Commission's view .....	37
THE DEFINITION OF CONSENT .....	42
The meaning of consent .....	42
Submissions .....	45
The Commission's view .....	47
RECOMMENDATIONS .....	51

### THE APPLICATION OF THE DRAFT BILL

#### The application of the draft Bill to all persons

4.1 The draft Bill provides both criminal and civil provisions for the regulation of the use of a surveillance device, and the communication or publication of information obtained from the use of a surveillance device.

4.2 The Commission is of the view that the legislation based on the draft Bill should apply to all persons, including the State (and also make it clear that the State cannot be prosecuted for an offence against the legislation).

#### Relationship with other laws

##### *The Information Privacy Act 2009*

4.3 The IP Act protects the personal information of individuals, generally through a set of 'privacy principles' that govern how Queensland Government agencies collect, store, use and disclose personal information.<sup>1</sup> It also allows an

<sup>1</sup>

Relevantly, an 'agency' is defined to mean a Minister, department, local government or public authority, and includes a body comprised within the agency: *Information Privacy Act 2009* (Qld) 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 that 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 the National Privacy Principles ('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').

individual to make a complaint about an agency's breach of the privacy principles.<sup>2</sup>

4.4 The draft Bill is intended to operate alongside the IP Act. Accordingly, the draft Bill provides that '[the legislation] does not affect the operation of the *Information Privacy Act 2009*'.

### **Other laws regulating the use of surveillance devices**

4.5 In Queensland, in addition to the general regulation of the use of a listening device under the *Invasion of Privacy Act 1971*, there are other Acts that separately regulate the use of one or more categories of surveillance devices for specific purposes. These Acts include:

- the PPRA, which establishes procedures for police to obtain a warrant or emergency authorisation for the use of a listening device, an optical surveillance device, a tracking device or a data surveillance device in the criminal investigation of a relevant offence;<sup>3</sup>
- the *Crime and Corruption Act 2001*, which regulates the use of a listening device, an optical surveillance device, a tracking device or a data surveillance device by authorised officers of the Crime and Corruption Commission;<sup>4</sup>
- the *Commissions of Inquiry Act 1950*, which authorises the use of a listening device, on the approval of a Supreme Court judge;<sup>5</sup>
- the *Public Safety Preservation Act 1986*, which authorises a police officer to use a surveillance device in certain emergency circumstances;<sup>6</sup> and
- the *Fisheries Act 1994*, which authorises an inspector to use a body-worn camera to record images or sounds while exercising a power under the Act.<sup>7</sup>

4.6 Some of the authorising provisions under these Acts are for the purposes of enforcing a State law, whilst others are for the protection of members of the public

<sup>2</sup> *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 NPPs, which are set out in sch 4 of the Act.

<sup>3</sup> *Police Powers and Responsibilities Act 2000* ch 13. Chapter 13 of the PPRA is not intended to affect other Queensland laws that prohibit or regulate the use of surveillance devices entirely within Queensland: s 325(1). Generally, a 'relevant offence' is an indictable offence for which the maximum penalty is at least seven years imprisonment, or an offence included in schedule 2 of the Act. In relation to an application for a warrant that authorises the use of a tracking device only and does not authorise covert entry to a building by the person installing it, or a warrant of that type, a 'relevant offence' is an indictable offence for which the maximum penalty is at least three years imprisonment, or an offence included in schedule 2 of the Act: s 323(1)–(3). Schedule 2 includes, for example, some offences that relate to objectionable computer games or films, child exploitation material, prostitution, racing integrity and weapons.

See also s 609A, which authorises a police officer to wear a body-worn camera to record images or sounds while the officer is acting in the performance of the officers' duties.

<sup>4</sup> *Crime and Corruption Act 2001* (Qld) ch 3 pt 6. The Act provides a process for obtaining a warrant to use a surveillance device in particular circumstances.

<sup>5</sup> *Commissions of Inquiry Act 1950* (Qld) s 19C.

<sup>6</sup> *Public Safety Preservation Act 1986* (Qld) pt 3B.

<sup>7</sup> *Fisheries Act 1994* (Qld) s 181A.

or of the safety of public officers or other authorised persons in the performance of their functions.

4.7 The Commission is of the view that the draft Bill should not affect the operation of another law regulating the use of surveillance devices. Accordingly, a provision to this effect is included in the draft Bill.

4.8 The separate regulation of the use of surveillance devices is also recognised in the draft Bill through the operation of the exception for the use of a surveillance device that is authorised under another Act. This exception applies in relation to the use prohibitions and the communication or publication prohibitions.<sup>8</sup> Where a person uses, or communicates or publishes information obtained from the use of, a surveillance device in a way that is authorised under another Act, this exception will apply and the use, communication or publication in those circumstances will not be unlawful under the draft Bill.

***Laws regulating the use of surveillance devices for State law enforcement purposes***

4.9 The terms of reference exclude from the scope of this review ‘Queensland’s existing laws regulating the use of surveillance devices for State law enforcement purposes’.<sup>9</sup> In this regard, the terms of reference explain that:

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.

4.10 The draft Bill provides that it is not an offence to use a surveillance device where the use is authorised under another Act. Accordingly, the operation of a law regulating the use of a surveillance device (including a law under which a surveillance device is used for a ‘State law enforcement purpose’) will not be affected by the draft Bill.

4.11 In particular, the PPRA separately regulates the use of surveillance devices in criminal investigations of relevant offences.<sup>10</sup> Under that Act, police officers may obtain a warrant or an authorisation to use surveillance devices in particular circumstances and for particular purposes.<sup>11</sup>

4.12 At present, police officers are also assisted in their activities by recordings made outside the scope of the PPRA by individuals using surveillance devices. Under the *Invasion of Privacy Act 1971*, it is lawful for a person who is a party to a

---

<sup>8</sup> See [5.339] ff and [6.116] ff below. The exceptions to the civil obligations not to interfere with an individual’s surveillance privacy also include the circumstance in which the use, communication or publication was authorised or required by law or by an order or a process of a court: see [8.95]–[8.100] below.

<sup>9</sup> Terms of reference, para E in Appendix A.

<sup>10</sup> The functions of the Queensland Police Service include protecting the community, preventing crime, and detecting offenders and bringing them to justice: *Police Service Administration Act 1990* (Qld) s 2.4.

<sup>11</sup> Police officers may also use a listening device (or another surveillance device) in ways that are not prohibited by the *Invasion of Privacy Act 1971*, or by other laws.

private conversation to use a listening device to record the conversation, without the other party's consent. Among other things, a person who was the victim of or a witness to a criminal offence might record a conversation that they have with the alleged offender, without that person's consent, in order to gather evidence or obtain corroboration of their version of events.

4.13 The regulation of the use of surveillance devices under the draft Bill is based on different principles and policy settings from the *Invasion of Privacy Act 1971*. In particular, the draft Bill does not retain participant monitoring, but instead includes a number of general purpose-based exceptions.<sup>12</sup>

4.14 This will have an impact on the circumstances in which a listening device, or other surveillance device, may be used by an individual without consent to provide information or evidence to assist with police inquiries or investigations.<sup>13</sup>

4.15 Relevant exceptions under the draft Bill that permit the use, installation or maintenance of a surveillance device include use that is: reasonably necessary to protect a person's lawful interests or in the public interest; or to obtain evidence of, or information about, a serious threat to a person's life, health, safety or wellbeing, or a serious threat of substantial damage to property.<sup>14</sup>

4.16 The draft Bill does not otherwise include specific exceptions for the use of surveillance devices, without consent, by police or other public officers for State law enforcement purposes. The regulation of such use raises policy questions that should be considered in the specific context of their own legislation, and which fall outside the scope of this review.

## THE DEFINITION OF SURVEILLANCE DEVICE AND RELATED DEFINITIONS

4.17 A fundamental question for the review is what approach should be taken to defining surveillance devices.

4.18 In the Consultation Paper, the Commission sought submissions on whether the legislation should adopt the existing 'recognised categories' approach used in other jurisdictions, or adopt an alternative 'technology neutral' approach.<sup>15</sup>

### Approaches to the definition of surveillance device

#### *Recognised categories approach*

4.19 The current approach of surveillance devices legislation is to regulate recognised categories of surveillance devices (that is, a listening device, an optical

---

<sup>12</sup> See [5.238] ff below.

<sup>13</sup> The use of a surveillance device, and the subsequent communication or publication of any information obtained, will not always be prohibited by the *Invasion of Privacy Act 1971* or the draft Bill. For example, use of a security camera by a business or a dashboard camera by an individual, and the communication or publication of information captured, is generally not prohibited unless it relates to a private conversation or a private activity.

<sup>14</sup> See [5.254] ff below. Similar exceptions apply to the communication or publication of surveillance information: See [6.69] ff below.

<sup>15</sup> QLRC Consultation Paper No 77 (2018) Q-3 to Q-5.

surveillance device, a tracking device and a data surveillance device). These categories are defined by reference to the general function or capability of the device (for example, a device that can be used to listen to, observe, monitor, record, or record visually).<sup>16</sup>

### ***Alternative technology neutral approaches***

4.20 Some law reform commissions have considered that surveillance devices legislation should adopt a broad ‘technology neutral’ approach.<sup>17</sup>

4.21 The NSWLRC recommended that ‘surveillance device’ should be defined broadly to mean:<sup>18</sup>

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

4.22 It also recommended that:<sup>19</sup>

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.

4.23 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’.<sup>20</sup> The ALRC recommended 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, an optical surveillance device, a tracking device or a 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’.<sup>21</sup>

<sup>16</sup> See further [2.20], [2.29] above.

<sup>17</sup> See further QLRC Consultation Paper No 77 (2018) [3.33] ff. The existing recognised categories approach is sometimes described as ‘technology neutral’ or ‘non-device specific’ to the extent that it applies to widely defined categories of devices without being limited to specific types of technologies.

<sup>18</sup> NSWLRC Interim Report No 98 (2001) [2.15]–[2.19], [2.33]–[2.36], Rec 1, endorsed in NSWLRC Report No 108 (2005) [1.21].

<sup>19</sup> NSWLRC Interim Report No 98 (2001) [2.37]–[2.39], Recs 2, 3. See further QLRC Consultation Paper No 77 (2018) [3.36]–[3.37]. The NSWLRC explained that those definitions are ‘deliberately circular so as to exclude the use of a surveillance device for purposes other than conducting surveillance’: NSWLRC Report 108 (2005) [1.8]. In this context it noted that, for an activity to constitute surveillance it must comprise the following elements: the use of a surveillance device; where there is a deliberate intention to monitor a person, place, etc; for the purpose of obtaining information about the surveillance subject: [1.8], [3.4].

<sup>20</sup> ALRC Report No 123 (2014) [14.32], Rec 14-2.

<sup>21</sup> Ibid [14.32], [14.39].

4.24 The ALRC noted that, given this approach, the offences would need to be appropriately tailored so that ‘an offence would only be made out where the particular use of the device is inappropriate’.<sup>22</sup>

4.25 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.

4.26 Where jurisdictions have reformed their surveillance devices legislation, the existing recognised categories approach has been retained, with reforms to expand the range of categories beyond listening devices and to modernise other aspects of the legislation.<sup>23</sup> This approach was also recommended in the recent ACT Review.<sup>24</sup>

## Submissions

4.27 Most respondents considered that it is necessary for the legislation to keep pace with existing and emerging technologies. However, views differed as to how this is best achieved.

4.28 Several respondents, including the OIC, submitted that the legislation should adopt the recognised categories approach, consistently with surveillance devices legislation in other jurisdictions.<sup>25</sup> A number of those respondents stated that consistency with other jurisdictions is important and desirable.<sup>26</sup>

4.29 Some respondents submitted that the recognised categories approach reduces ambiguity and provides certainty as to the scope of the legislation.<sup>27</sup> The OIC submitted that:

[w]hile privacy laws should be sufficiently flexible to adapt to rapidly changing technologies and capabilities, ‘laws should be drafted with sufficient precision and definition to promote certainty as to their application and interpretation’.<sup>28</sup> In the absence of a clear statutory definition, the scope of the Bill will be uncertain and potentially open to challenge.

Further, failure to sufficiently define the meaning of ‘surveillance device’ in the legislation could lead to a range of unintended consequences given the broad range of devices with surveillance capabilities that can be used for legitimate

---

22 Ibid [14.41].

23 See, eg, the *Surveillance Devices Act 2007* (NSW), which replaced the *Listening Devices Act 1984* (NSW). See also [2.28] ff above.

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

25 Eg, Submissions 13, 15, 19, 36, 38.

26 Eg, Submissions 15, 19, 35, 38. The OIC, referring to ALRC Report No 123 (2014) 197 and [2.37], noted that:

This aligns with the view expressed by the ALRC ... that ‘consistency and uniformity in surveillance device laws ... is desirable’. The ALRC noted that ‘laws that are unnecessarily complex, fragmented and inconsistent impose an unnecessary regulatory burden on business. They also harm privacy ... cause uncertainty and confusion, and make the law less effective’.

27 Eg, Submission 38. Also Submission 43.

28 ALRC Report No 123 (2014) [2.30].



purposes and are outside the intended scope of the regulatory framework. (note in original)

4.30 The Department of Agriculture and Fisheries similarly noted that any ambiguity in the definition of a surveillance device would ‘cause uncertainty and may lead to a person doing an unlawful act of surveillance without knowing’.

4.31 Some respondents generally submitted that each category of device (that is, a listening device, an optical surveillance device, a tracking device and a data surveillance device) should be defined broadly and consistently with the legislation in other jurisdictions.<sup>29</sup>

4.32 Several respondents, including an academic and DTMR, also noted that the definition of each category should extend to programs and systems.<sup>30</sup> In contrast, the Department of Agriculture and Fisheries submitted that this extended definition would be relevant for data surveillance devices, but may not relate to other categories of devices.

4.33 DTMR suggested that another category of device could be ‘any device that is capable of recording personally identifiable information’ in order to ‘cover any emerging technology’. The QCCL similarly submitted that the definition of ‘surveillance device’ should include ‘any technological means to correlating identity data’, that is, ‘personal information’ within the meaning of the IP Act.

4.34 Some respondents also submitted that the definition of ‘surveillance device’ should include a combination of two or more of the categories of devices or technologies.<sup>31</sup> However, some observed that the recognised categories approach may give rise to difficulty or uncertainty where a device falls into more than one category.<sup>32</sup>

4.35 In addition, some respondents submitted that the legislation should enable other surveillance devices or technologies to be prescribed by regulation.<sup>33</sup> The OIC stated that:

Surveillance technologies continue to evolve and any legislative definition must ensure that it encompasses future advances in these technologies. In OIC’s view, enabling other devices to be prescribed by regulation provides the legislative framework with sufficient flexibility to keep pace with emerging surveillance technologies.

4.36 However, DTMR observed that ‘this approach has limitations’. First, the mechanism is reactive rather than proactive and requires the government to respond in a timely way to rapid technological developments. Second, there is a risk that a

---

<sup>29</sup> Eg, Submissions 19, 36, 38.

<sup>30</sup> Eg, Submissions 19, 36.

<sup>31</sup> Eg, Submissions 13, 36.

<sup>32</sup> Eg, Submission 35.

<sup>33</sup> Eg, Submissions 13, 36, 38.

new type of device added by regulation may not fit in to the broader legislative regime.<sup>34</sup>

4.37 In contrast, several respondents submitted that the legislation should adopt a broad ‘technology neutral’ approach.<sup>35</sup>

4.38 Those respondents generally observed that a technology neutral approach would cover existing and emerging technologies.<sup>36</sup> QAI stated that:

with continually emerging technology, it will be challenging to develop and maintain an exhaustive list of categories. Further, certain emerging technologies (such as biometrics) that have a wide scope for surveillance may be difficult to track. We submit that, in light of rapid technological development, it is more appropriate to adopt a ‘technology neutral’ approach ...

4.39 The Chief Magistrate noted that ‘regulation of surveillance should not be device specific to ensure that the law is not outpaced by technological developments’.

4.40 A member of the public similarly noted that the main argument for supporting a technology neutral approach is that technology capable of being used for surveillance has proliferated, is widespread and is undergoing constant development. That respondent observed that a technology neutral approach would ‘ensure that the pace of innovation in technologies that can be used or re-purposed for surveillance does not render any new law immediately obsolete’.<sup>37</sup>

4.41 The AAUS stated that:<sup>38</sup>

The growth and increased sophistication of modern surveillance devices not only makes it imperative to introduce some legislative control on their installation and use, but also makes it necessary to define such devices broadly so as to accommodate for current and future technologies. Any definition of the term ‘surveillance device’ should therefore be technology neutral, that is, the rules ‘should neither require nor assume a particular technology’. (notes omitted)

4.42 A few respondents expressed support for a broad definition of ‘surveillance device’, such as:<sup>39</sup>

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.

---

<sup>34</sup> The OIC also noted the risk that ‘the effectiveness of this approach requires ongoing monitoring by the legislature’.

<sup>35</sup> Eg, Submissions 10, 18, 22, 24, 27, 29, 30, 33, 35, 39, 40, 43.

<sup>36</sup> Eg, Submissions 10, 16, 29, 30, 33, 35, 39. A government department noted that ‘[r]estrictive definitions risks not to encapsulate new technology’: Submission 16.

<sup>37</sup> Submission 29.

<sup>38</sup> AAUS and Liberty Victoria Paper (2015) [4.2], adopted in Submission 39 from the AAUS.

<sup>39</sup> Eg, Submissions 10, 18, 27, 33, 40. See QLRC Consultation Paper No 77 (2018) Q-5.

4.43 However, a member of the public expressed concern that this definition gives too much emphasis to the notion of ‘deliberate’ monitoring of a person or object and insufficient emphasis to the consequences of monitoring on the privacy of others impacted by the surveillance.<sup>40</sup>

For example, Person A may mount a surveillance device (digital audio-visual camera) on a tall pole attached to their residential property boundary fence for the stated purpose of ‘monitoring their dog’ and/or their private property. In doing so, because of the position of the digital camera (i.e. on a tall pole attached to a property boundary fence), and capability of the digital camera (i.e. wide visual field and audio), they also consequently capture and record the private property, private conversations and private activities of their neighbour (Person B). Under the proposed definition [set out at [4.42] above] in Q-5 [of the Consultation Paper], the neighbour (Person B), who has expressly not consented to the surveillance of their private place, persons, conversations or activities, may have no recourse or protection under the proposed legislation. This is because Person A could argue they are not ‘deliberately’ monitoring Person B, they are monitoring for the purposes of protecting their dog/property. The privacy interests of Person B may not be sufficiently protected by this definition if adopted in the proposed new legislation.

4.44 The AAUS suggested that ‘surveillance device’ should be defined broadly to mean ‘any device capable of being used to’:<sup>41</sup>

- (a) monitor, observe, overhear, listen to or record an activity; or
- (b) determine or monitor the geographical location of a person or an object.

4.45 While the QLS supported a broad technology neutral definition of surveillance device, it also noted generally that ‘[p]articular care is required in the drafting of any legislation to ensure that its reasonable interpretation is clear, and consistently applied by all relying on it’.

4.46 A government department similarly noted that ‘any legislation would need to be carefully drafted to include all permitted uses and reduce ambiguity’.<sup>42</sup>

## **The Commission’s view**

### ***Definition of ‘surveillance device’ and ‘surveillance information’***

4.47 The draft Bill adopts the recognised categories approach to defining the term ‘surveillance device’ and related terms. The purpose of the draft Bill is to protect an individual’s privacy from unjustified interference from the use, and the communication or publication of information obtained from the use, of surveillance devices.<sup>43</sup> It is important that the definition of ‘surveillance device’ is clear, so that the legislation is capable of enforcement. This approach also achieves reasonable consistency with surveillance devices legislation in other jurisdictions.

---

<sup>40</sup> Submission 13.

<sup>41</sup> AAUS and Liberty Victoria Paper (2015) [4.2], Rec 2, adopted in Submission 39 from the AAUS.

<sup>42</sup> Submission 16.

<sup>43</sup> See further [3.26] above.

4.48 In contrast, a broad technology neutral approach, which focuses on activities rather than devices, would make the identification of all the activities to be protected more complex. Privacy is multifaceted and difficult to define, and there are many legitimate reasons for the use of a surveillance device. A broad technology neutral approach may have the unintended consequence of making activities that are not presently regulated the subject of regulation and potential criminal liability.

4.49 There is also a need for the legislation to differentiate between different devices, particularly in relation to the criminal offences. The draft Bill generally provides that it is an offence to use a surveillance device, or to communicate or publish information obtained from such use, without consent. The individual whose consent is relevant varies between the different categories of device, as different devices give rise to different privacy concerns and considerations. The recognised categories approach enables the consent element for each of the criminal offences to be linked to the individual whose privacy interests are affected.<sup>44</sup>

4.50 The draft Bill defines a 'surveillance device' as a listening device, an optical surveillance device, a tracking device and a data surveillance device. The definition of each category of device is discussed below.

4.51 The draft Bill also provides that a 'surveillance device' is a device that is a combination of two or more of the defined categories of devices. This recognises that there are many devices that fit into two or more categories. For example, a video camera often has an audio recording capability and can be used as both a listening device and an optical surveillance device. In such cases, the applicable offence or offences will turn on the facts of each case, including how the device was actually used and what information was obtained.

4.52 The draft Bill defines the term 'surveillance information' to mean information obtained, directly or indirectly, using a surveillance device. It also broadly defines the term 'information' to include a record in any form and a document.

4.53 The Commission acknowledges that, if implemented, the legislation based on the draft Bill will need to be kept under review in light of developments in surveillance device technology and the use of surveillance devices.<sup>45</sup> However, it considers that the overriding need is for certainty in relation to the scope and application of the legislation, particularly as it will create criminal offences.

4.54 An emerging area that may require further consideration as technology develops is biometric surveillance. Presently, biometric technology is sometimes used for the purposes of identification and authentication. In some cases, biometric technology such as fingerprint scanning may be used as a means of tracking an

---

44 In relation to an optical surveillance device, for example, consent is required from each of the parties to a private activity. However, in relation to a data surveillance device, consent is required from each person who owns, or is in lawful control of, a computer. For a discussion of whose consent is required in relation to each category of device, see [5.204] ff below.

45 One of the functions of the proposed new regulator under the draft Bill is to monitor whether the legislation is achieving its purpose, how surveillance devices and surveillance device technologies are used in civil society, and developments in surveillance device technology: see [10.113]–[10.114] and Rec 10-12(a) below. The draft Bill also requires the legislation to be reviewed within five years after its commencement: see [11.3]–[11.5] and Rec 11-2 below.

individual's location. To that extent, it is capable of falling within the scope of a 'tracking device', as defined in the draft Bill. As technology develops and the capabilities of biometric surveillance increase, how it should be regulated in the context of its use in civil society may need further consideration.

### ***Definition of each category of device***

4.55 The draft Bill defines each category of device included in the definition of surveillance device broadly by reference to its general function or capability (for example, a device that can be used to listen, observe, monitor, record or record visually). This provides some flexibility and will ensure that, as far as practicable, the draft Bill will apply to emerging devices with those capabilities.

4.56 The definitions for each category of surveillance device are consistent with surveillance devices legislation in other jurisdictions and with the PPRA.<sup>46</sup>

### ***Definition of a 'listening device'***

4.57 The draft Bill defines a 'listening device' as a device capable of being used to listen to, monitor or record, words spoken to, or by, an individual in a conversation. This will include, for example, a bugging device.

4.58 The draft Bill is not intended to apply to the use of a device by an individual with a hearing impairment to enable them to hear sounds ordinarily audible to the human ear. To make this clear, the definition expressly excludes a hearing aid or similar device used by an individual with impaired hearing.

### ***Definition of an 'optical surveillance device'***

4.59 The draft Bill defines an 'optical surveillance device' as a device capable of being used to observe, monitor or visually record an activity. This will include, for example, a camera, video camera, drone or other device with those capabilities.

4.60 However, as is the case with listening devices, the draft Bill is not intended to apply to the use of a device by an individual with a vision impairment to enable them to see sights ordinarily visible to the human eye. The definition should therefore expressly exclude spectacles, contact lenses or a similar device used by an individual with impaired vision.

### ***Definition of a 'tracking device'***

4.61 The draft Bill defines a 'tracking device' as a device capable of being used to find, monitor or record the geographical location of an individual, vehicle or other thing.

---

<sup>46</sup>

See [2.27]–[2.31] above; *Police Powers and Responsibilities Act 2000* (Qld) s 322 (definitions of 'data surveillance device', 'optical surveillance device', 'surveillance device', 'tracking device'), sch 6 (definition of 'listening device').

4.62 The most common examples of a tracking device use the Global Positioning System ('GPS') to determine a geographical location.<sup>47</sup> They include a specific GPS logger and a smartphone that has GPS capability.

**Definition of a 'data surveillance device'**

4.63 The draft Bill defines a 'data surveillance device' as a device or program capable of being used to access, monitor or record information that is input into, output from, or stored in a computer. It further defines 'computer' as an electronic device for storing and processing information.

4.64 The Commission considers that the definition of data surveillance device should include a program as well as a device. The term 'program', as used in relation to a computer, is intended to have its ordinary meaning of 'a set of instructions written in an artificial language which a computer can interpret and execute'.<sup>48</sup> It is therefore not necessary for the term to be defined in the draft Bill.

4.65 A common example of a data surveillance device is a keylogger, which monitors or records keystrokes as they are made and can be used to obtain sensitive information such as passwords, banking or credit card details, or personal messages. Keyloggers include a physical device and a program that is installed when a person opens an attachment or downloads a file in an email.

4.66 South Australia is currently the only Australian jurisdiction that regulates the use of a data surveillance device to access, track, monitor or record information stored in a computer.<sup>49</sup>

4.67 The prohibition relating to the use of a data surveillance device without consent may, in some cases, overlap with existing offences under the *Telecommunications (Interception) Access Act 1979* (Cth) and the Criminal Code prohibiting accessing or 'hacking' information stored in a computer.<sup>50</sup> However, the Commission considers that surveillance devices legislation should also provide protection in relation to the use of a data surveillance device to access information stored in a computer.

**Scope of regulation of surveillance devices under the draft Bill**

4.68 The Commission notes that many common devices are capable of being used as a surveillance device, such as a smartphone. However, the provisions in the draft Bill do not apply to every use of a surveillance device. Although the definition of a surveillance device and each category of surveillance device is cast broadly, the

---

<sup>47</sup> A 'geographical location' is a specific physical point on earth, which is often defined by coordinates of latitude and longitude.

<sup>48</sup> Macquarie Dictionary (online at 20 January 2020) 'program'.

<sup>49</sup> *Surveillance Devices Act 2016* (SA) s 8(1). Surveillance devices legislation in all other jurisdictions defines a 'data surveillance device' to mean a device that can be used to monitor or record the *input of information into or output of information* from a computer (emphasis added): see [2.29] above.

<sup>50</sup> See further the discussion of the relevant offences under the *Telecommunications (Interception) Access Act 1979* (Cth) and the Criminal Code (Qld) at [D.9]–[D.11], [D.44] below.

draft Bill regulates such devices only in particular circumstances, as prescribed by the criminal prohibitions and the civil law provisions.

4.69 The criminal prohibitions apply only when a surveillance device is being used without consent as follows (and where an exception does not apply):<sup>51</sup>

- for *listening devices*—to listen to, monitor or record a private conversation;
- for *optical surveillance devices*—to observe, monitor or visually record a private activity;
- for *tracking devices*—to find, monitor or record the geographical location of an individual or a vehicle or other thing; or
- for *data surveillance devices*—to access, monitor or record information that is input into, output from or stored in a computer.

4.70 The civil law provisions dealing with the general obligations apply only where a surveillance device is used without consent in a way that interferes with an individual's surveillance privacy (and where an exception does not apply).<sup>52</sup>

4.71 In relation to tracking devices and data surveillance devices, the Commission notes that a large amount of data, including location data, is generated and collected about individuals online from the use of devices, such as computers, smartphones and fitness trackers.

4.72 While this gives rise to privacy considerations and concerns, the collection, storage, use and protection of such data is not the subject of surveillance devices legislation. For some entities, those matters are regulated by the IP Act and the Privacy Act.<sup>53</sup>

4.73 The ACCC recently completed an inquiry into digital platforms, including how they collect, use and disclose user data.<sup>54</sup> In particular, it examined three data practices of particular concern to consumers: the collection of location data, online tracking of consumers for targeted advertising purposes, and the sharing of user data with third parties.<sup>55</sup> The ACCC made a number of recommendations to enhance

<sup>51</sup> See further the discussion of the use prohibitions and the communication or publication prohibitions in Chapters 5 and 6 below. The meaning of 'private conversation' and 'private activity' and the role of consent are discussed in Chapter 5.

<sup>52</sup> See further Chapter 8 below.

<sup>53</sup> See further [D.18]–[D.31] below.

<sup>54</sup> The ACCC examined the intersection of privacy, competition and consumer protection considerations in relation to digital platforms. 'Digital platforms' are 'applications that serve multiple groups of users at once, providing value to each group based on the presence of other users'. Common examples of digital platforms include social media platforms' such as Facebook, online search engines, such as Google and digital content aggregation platforms such as Apple News: ACCC Digital Platforms Inquiry Report (2019) [1.1], [7.8.1] 41 ff. The ACCC noted that the information collected goes beyond what a user actively provides while they are using a digital platform's services. It also includes data about the user that is passively collected (for example, by background collection of location data) or inferred from other sources by analysing or aggregating datasets. It also noted that digital platforms also often have broad discretions in how they use and disclose this data, and identified issues with obtaining meaningful consent and with consumers having meaningful control over their data: *ibid* [7.12] ff.

<sup>55</sup> ACCC Digital Platforms Inquiry Report (2019) [7.3] ff.

privacy and data protections, including recommending amendments to extend the Privacy Act to include user data collected by digital platforms.<sup>56</sup>

4.74 The Commission also notes that individuals often choose to share or make their personal information available online. They may, for example, make their location known by ‘checking in’ to a place online, or by using an application that enables others to find their phone. Someone else may utilise such information to track the individual’s location or activities. However, surveillance devices legislation is not intended to apply to the use of information a person has made publicly available.

## THE DEFINITION OF CONSENT

4.75 Consent is a key element of the draft Bill.<sup>57</sup> The Commission has considered whether, and if so how, consent should be defined.

### The meaning of consent

4.76 In the context of privacy law, consent is generally understood as having a number of components, namely, that:<sup>58</sup>

- an individual has capacity to give or refuse consent, which includes the individual being able to understand the nature and effect of their decision, form a view that is based on reasoned judgment and communicate their consent;<sup>59</sup>
- consent is informed, including by having enough information to be able to understand the intent and purpose of the consent that is sought, how any relevant information will be handled, and the consequences of giving or refusing consent;<sup>60</sup>

<sup>56</sup> Ibid 456 ff, Rec 16. The ACCC also recommended that consideration be given to broader reform of Australian privacy law to address gaps in the regulatory framework, the introduction of an enforceable privacy code for digital platforms, and the introduction of a statutory tort for serious invasions of privacy: *ibid* 476 ff, Recs 17-19. The Government has announced that it will introduce draft legislation to amend the Privacy Act, including to introduce a binding privacy code of practice, to be developed by the OAIC, in 2020. It has also committed to undertake a broader review of the Privacy Act, to be completed in 2021: Australian Government, ‘Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry’ (2019).

<sup>57</sup> See [3.18] above.

<sup>58</sup> See especially OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.0]; OAIC Guideline: Key concepts—Consent (2019) [B.35]; ALRC Report No 108 (2008) [19.9], [19.11], [19.60]; VLRC Report No 18 (2010) [6.15], citing Jeremy Douglas-Stewart, *Annotated National Privacy Principles* (2007). See also, generally, ACCC Digital Platforms Inquiry Report (2019) [7.4], Rec 16(c).

<sup>59</sup> See especially OAIC Guideline: Key concepts—Consent (2019) [B.52]; OAIC, *Consent to the handling of personal information* <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/>>; OAIC, *Disclosing information about patients with impaired capacity* (2019) 2.

<sup>60</sup> See especially OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.3]; OAIC Guideline: Key concepts—Consent (2019) [B.47].



- consent is given freely and voluntarily, meaning that an individual has a ‘genuine opportunity’ to give or refuse consent and is not, for example, tricked into agreeing;<sup>61</sup> and
- consent is current and specific to the particular circumstances or matter in question.<sup>62</sup>

4.77 An individual might not have capacity to consent because of factors such as age, illness or disability. In determining capacity, relevant matters may include whether the individual has currently or previously expressed their views and opinions, and whether they could be given support to have capacity or to be involved in decision-making.<sup>63</sup> Where an individual does not have capacity, other laws may apply.<sup>64</sup>

### **Surveillance devices legislation**

4.78 The surveillance devices legislation in each jurisdiction includes consent as an element of the criminal prohibitions or as an exception to the criminal prohibitions. The legislation provides that consent may be express or implied.<sup>65</sup>

4.79 The terms ‘express’ and ‘implied’ consent are not defined by surveillance devices legislation. Generally, express consent will exist where an individual provides clear or explicit consent.<sup>66</sup> For example, in relation to a private conversation between two individuals, express consent would exist where one individual makes a

<sup>61</sup> See, in particular, OAIC Guideline: Key concepts—Consent (2019) [B.43]–[B.44]; OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.2]; OAIC, *Consent to the handling of personal information* <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/>>.

<sup>62</sup> See, in particular, OAIC Guideline: Key concepts—Consent (2019) [B.48]; OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.4]–[4.5]; OAIC, *Consent to the handling of personal information* <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/>>. People should also be informed of their ability to withdraw consent.

<sup>63</sup> OAIC Guideline: Key concepts—Consent (2019) [B.53]–[B.55], [D.33]–[D.34]; OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.1]. These guidelines state generally that if a person does not have capacity, someone else may act on their behalf but the person should still be involved in decision-making.

<sup>64</sup> See further [4.108] ff below.

<sup>65</sup> In the Australian Capital Territory, ‘consent’ is defined to include implied consent. In other jurisdictions, the concept of express or implied consent is incorporated into relevant sections of the legislation. See *Invasion of Privacy Act 1971* (Qld) ss 4 (definition of ‘private conversation’), 42(2)(b), 44(2)(a)(i), 45(2)(a); *Listening Devices Act 1992* (ACT) s 2, Dictionary (definition of ‘consent’); *Surveillance Devices Act 2007* (NSW) ss 4(1) (definitions of ‘party’ and ‘private conversation’), 7(3)(a), 8(1), 9(1), 10(1), 11(2)(a)(ii), 12(2)(b), 14(2)(a)(ii); *Surveillance Devices Act* (NT) ss 11(1)(b), (2)(b)(i), 12(1)(b), 13(1)(b), 14(1)(b), 15(2)(a), 16(2)(a); *Surveillance Devices Act 2016* (SA) ss 4(2)(a)(i), 5(1)–(3), 7(1), 8(1); *Listening Devices Act 1991* (Tas) ss 3(1) (definitions of ‘party’ and ‘private conversation’), 5(3)(a), 9(2)(a)(ii), 10(2)(a), 11(2)(b); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1), 9(1), 11(2)(a), 12(2)(a); *Surveillance Devices Act 1998* (WA) ss 3(1) (definition of ‘party’), 5(3)(c), (d), 6(3)(a), (b), 7(1), 9(2)(a)(ii), 26(1), (2), 27(1), (2).

There are some instances where consent is not identified as being express or implied: see, eg, *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening Devices Act 1991* (Tas) s 5(3)(b); *Surveillance Devices Act 1999* (Vic) s 6(2)(c)(i).

In South Australia, the concept of express or implied consent is included in provisions about the use of surveillance devices, but provisions about the communication or publication of information refer only to ‘consent’. The definition of ‘public place’ refers to ‘express or tacit consent’: s 3(1) (definition of ‘public place’).

<sup>66</sup> See, eg, OAIC Guideline: Key concepts—Consent (2019) [B.36]; OAIC, *Consent to the handling of personal information* <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information/>>.

request to record the conversation or to publish an account of the conversation in a newspaper article, and the other individual agrees to the request.

4.80 Generally, consent may be implied where an individual has not given express consent, but their conduct and the surrounding circumstances can be relied on to demonstrate their consent. The VLRC used the term ‘implied consent’ to mean ‘behaviour falling short of express agreement, which would cause a reasonable observer to conclude that the person has agreed to a particular course of conduct’.<sup>67</sup>

4.81 The IP Act and the Privacy Act define consent as express or implied consent, and the IPPs refer to express or implied agreement.<sup>68</sup> Guidelines issued by the OAIC explain that consent should not be assumed only because an individual did not object to a proposal, cannot be inferred simply because the individual was given notice, and ‘may not be implied if an individual’s intent is ambiguous or there is reasonable doubt about the individual’s intention’.<sup>69</sup>

4.82 In some circumstances, it may be difficult to determine whether consent is implied, and consent may not be ‘truly voluntary’ where an individual cannot, or cannot conveniently, choose not to be subject to surveillance.<sup>70</sup>

4.83 The VLRC<sup>71</sup> and the NSWLRC<sup>72</sup> both considered that legislation should

<sup>67</sup> VLRC Report No 18 (2010) [6.21], note 24.

In the context of the *Privacy Act 1988* (Cth), the OAIC describes implied consent as arising ‘where consent may reasonably be inferred in the circumstances from the conduct of the individuals and the APP entity’: OAIC Guideline: Key concepts—Consent (2019) [B.37].

In the context of the *Information Privacy Act 2009*, the OIC states that ‘[w]hether an individual has impliedly agreed is an objective test, to be determined by a reasonable inference from the individual’s actions’: OIC Guideline: Key privacy concepts—agreement and consent (2013) [5.0].

<sup>68</sup> *Information Privacy Act 2009* (Qld) IPPs 10(1)(a), (f)(iii), 11(1)(b), (f)(iii), sch 5 (definition of ‘consent’); *Privacy Act 1988* (Cth) s 6(1) (definition of ‘consent’). See also, generally, ACCC Digital Platforms Inquiry Report (2019), [7.4], Rec 16(c).

See generally, OIC Guideline: Key privacy concepts—agreement and consent (2013); OAIC Guideline: Key concepts—Consent (2019). The OIC guideline explains that ‘[t]he concepts of agreement and consent are not identical, but they are sufficiently similar that they can be explained together for the purposes of applying the IP Act’: [2.0].

The OIC and OAIC state in guidelines that agencies should generally seek express consent, particularly where information is sensitive’: OIC Guideline: Key privacy concepts—agreement and consent (2013) [5.0]; OAIC, *APP guidelines—consent* (22 July 2019) [B.41].

<sup>69</sup> OAIC Guideline: Key concepts—Consent (2019) [B.39]. The OAIC also explains that it would be difficult to establish that a person’s silence could be taken as consent. See also, generally, OAIC, *Consent to the handling of personal information* (8 August 2019).

<sup>70</sup> QLRC Consultation Paper No 77 (2018) [3.68]. See also, eg, M Paterson, ‘Regulating Surveillance: Suggestions for a Possible Way Forward’ (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 193.

<sup>71</sup> VLRC Report No 18 (2010) [6.21]. In its review of public place surveillance, the VLRC noted that implied consent is a ‘practical dividing line’ between behaviour in public places that is intrusive and undetectable, and behaviour that should be permitted because there have been reasonable attempts to alert the public. It also emphasised the importance of providing adequate notice of surveillance, such as appropriate signage. The VLRC also observed that consent is sometimes ‘conditional or restricted’, such as where a person consents to one type of surveillance, for example, the use of CCTV footage in a public place, but not to any form of surveillance that might occur in that place: VLRC Consultation Paper No 7 (2009) [3.90].

<sup>72</sup> NSWLRC, *Privacy principles*, Report No 123 (August 2009) [2.95]–[2.98]. In its review of privacy principles, the NSWLRC observed that suggested guidelines about consent should make it clear that a person ‘should endeavour to obtain express consent whenever practicable before relying on implied consent’: [2.98].

recognise express and implied consent. In particular, it was observed that the inclusion of implied consent is a practical approach, and that a requirement to obtain express consent might sometimes be impracticable or overly prescriptive. The ALRC came to a similar conclusion in the context of privacy law and the collection of sensitive information but ‘emphasised that implied consent must still be voluntary, informed, and obtained from a person with capacity to consent’.<sup>73</sup>

4.84 In contrast, the position taken in the ACT review was more closely aligned with a requirement for express consent.<sup>74</sup>

## Submissions

4.85 In the Consultation Paper, the Commission sought submissions on consent, including the circumstances in which a person should be able to use a surveillance device, or communicate or publish information obtained from the use of a surveillance device, with consent.<sup>75</sup>

4.86 Generally, respondents considered consent to be an important element of surveillance devices legislation. For example, Future Wise submitted that the ‘foundation principle of regulation’ should be that personal surveillance does not occur without ‘free, prior, and informed consent’. The Townsville Community Legal Service Inc. described ‘actual, informed consent’ as a ‘principal consideration’.

4.87 A number of respondents commented on the meaning or elements of consent. For example, the Department of Education submitted that consent should be ‘voluntary, informed, specific [and] current’, and QAI submitted that consent, for public place surveillance, should be ‘explicit, informed and free from undue influence’.<sup>76</sup> The Townsville Community Legal Service Inc. referred to ‘actual, informed consent’, and the QCCL referred to ‘informed consent’ as the preferred concept.<sup>77</sup>

4.88 The OIC submitted that surveillance should be permitted if it is with consent. However, the OIC also stated that consent is a complex concept, and noted that it has been criticised because ‘it is not always specific, informed and freely given due to a range of factors, including imbalance in bargaining power’.<sup>78</sup>

4.89 Some respondents observed that there are practical difficulties associated with requirements to obtain consent. The Department of Agriculture and Fisheries

<sup>73</sup> ALRC Report No 108 (2008), [22.69]–[22.70].

<sup>74</sup> ACT Review (2016) [2.5](e), [6.26], [6.30]. Among other things, it was stated that if the circumstances of a conversation or activity indicate that the parties intended it to be private, it ‘will generally preclude any implied consent’ and there will be a requirement for ‘additional evidence of consent beyond the objective circumstances of the surveillance by the parties involved’: [6.26].

<sup>75</sup> QLRC Consultation Paper No 77 (2018) Q-8, Q-16(a), Q-18(a).

<sup>76</sup> This respondent also referred, more generally, to ‘full, informed consent’ given by the person ‘without concern for any adverse consequences’.

<sup>77</sup> This respondent also referred, in particular, to ‘prior’ informed consent for public place surveillance.

<sup>78</sup> Citing ACCC, ‘Digital Platforms Inquiry’ (Preliminary Report, December 2018) 8, Rec 8(c), in which it was observed that the power imbalance between digital platforms and consumers, and common methods by digital platforms to obtain consent, limit consumers’ ability to ‘provide well-informed and freely given consent’ to data collection, use and disclosure.

submitted that consent requirements might be ‘unduly prohibitive’ and would ‘likely prevent effective surveillance’ in many cases, especially where timing is important. This respondent explained that, while it attempts to give notice when surveillance is likely to impact private properties, it would seek exemption from any requirement to obtain prior consent. The Insurance Council of Australia explained that, from an insurance perspective, it would be a challenge to obtain consent from individuals subject to surveillance. Claimants are unlikely to expressly consent to surveillance monitoring, and any consent given when a policy is issued would not be effective where the subject of the surveillance is a third party.

4.90 QAI, Future Wise and the Townsville Community Legal Service Inc. noted the need to consider the consent of vulnerable people, the latter submitting that ‘those most vulnerable are also often those from whom informed consent is most difficult to obtain’. The OIC noted that the issue of parental consent to surveillance poses additional challenges.

### ***Express and implied consent***

4.91 Respondents submitted that consent in surveillance devices legislation should incorporate both express and implied consent.<sup>79</sup>

4.92 The QCCL submitted that the concept of implied consent ‘should not be abandoned’, including because ‘there is much law behind the concept and it brings with it a level of flexibility’. This respondent suggested that the legislation should include two factors to be taken into account when considering whether consent is to be implied, namely:<sup>80</sup>

- (a) Whether or not adequate notice has been given of the use of the surveillance device.
- (b) Whether or not the person’s presence in the particular area where the surveillance device is in use, can truly be considered voluntary.

4.93 Respondents gave examples of implied consent, including where a person provides reasonable notice that a place is under surveillance and another person enters that place, or where a person is aware of, but does not object to, surveillance.<sup>81</sup> The Brisbane City Council observed that, for ‘indiscriminate optical surveillance’ of public places, signage is the ‘best means of alerting’ people to that surveillance because it is not feasible to obtain individual consent prior to entry.

4.94 A member of the public submitted that, to the extent it is possible, consent should be express, for example, verbally or in writing. Otherwise, as a minimum,

---

<sup>79</sup> Eg, Submissions 13, 19, 39, 40.

<sup>80</sup> Referring generally to VLRC Report No 18 (2010). In that report (at [6.15]–[6.23]), the VLRC observed that ‘implied consent’ can sometimes be difficult to characterise, but that it ‘remains the most practical dividing line’ for public place surveillance. It suggested that ‘adequate notice ... by signage or other means’ should be given.

<sup>81</sup> Eg, Submissions 13, 19. Cf [4.98] below.

consent should be implied.<sup>82</sup> Some respondents suggested that different types of consent might be suitable for different kinds of surveillance or surveillance devices.<sup>83</sup>

4.95 In contrast, another member of the public submitted that consent, in the context of the use prohibitions, should be express and not implied.<sup>84</sup>

### ***Consent to surveillance in a public place, and to overt or covert surveillance***

4.96 Some respondents considered consent in the context of surveillance in public or private places, or surveillance that is overt or covert.

4.97 A number of respondents submitted that, where surveillance devices are used in public places or are used overtly, there should be different requirements for the use of the devices. It was suggested, for example, that there should be clear notification about the use of surveillance devices, or that surveillance devices should be positioned in easily visible locations.<sup>85</sup>

4.98 However, other respondents expressed the view that, even where surveillance occurs in a public place, there should still be a requirement to obtain the express and informed consent of the person subject to surveillance.<sup>86</sup> The Townsville Community Legal Service Inc. stated that ‘whether one is aware of surveillance does not render the issue of consent null and void, nor does awareness or acquiescence provide an automatic acceptance’. In its view, the impact of a breach of privacy may not differ depending upon whether surveillance is overt or covert. The QCCL submitted that a requirement for consent would address the ‘asymmetric relationship’ that exists between the user of a surveillance device and the person subject to surveillance.<sup>87</sup>

## **The Commission’s view**

### ***The definition of consent***

4.99 The Commission’s starting point is that the use of a surveillance device, or the communication or publication of information obtained from the use of a surveillance device, is generally unlawful in the absence of consent.<sup>88</sup>

4.100 The Commission is of the view that the draft Bill should define consent to mean ‘express or implied consent’. The requirements for consent (namely, that the

<sup>82</sup> Submission 13.

<sup>83</sup> See [5.34] ff below and, eg, Submissions 13, 15, 35.

<sup>84</sup> Submission 22.

<sup>85</sup> Eg, Submissions 10, 13, 18, 25, 35, 38, 40. In contrast, another respondent submitted that notification of surveillance in a public place does not ‘legitimise’ that surveillance and impacts on notions of implied consent, including because a notice may not be seen and because people are put into a ‘no-win situation’, where they must either be subject to surveillance or leave the public place: Submission 17.

<sup>86</sup> Eg, Submissions 33, 40, 41. Also, eg, Submission 25, which suggested requirements for both consent to the recording of a person or their data as well as clear and explicit disclosure of surveillance in public spaces.

<sup>87</sup> Citing British Columbia Civil Liberties Association, ‘Video surveillance in public places’ (1999) <[https://bcccla.org/our\\_work/video-surveillance-in-public-places/](https://bcccla.org/our_work/video-surveillance-in-public-places/)>.

<sup>88</sup> See the discussion of the criminal prohibitions in Chapters 5 and 6 and the general obligations in Chapter 8 below.

individual has capacity, and that their consent is informed, free and voluntary, current and specific) are generally understood, and need not be included in the definition. Those requirements must be satisfied for a person's consent to be effective, whether it is given as express or implied consent.<sup>89</sup>

4.101 This approach is consistent with surveillance devices legislation in other jurisdictions, and with the IP Act and the Privacy Act. In relation to the latter Acts, consent is explained in detail in guidelines and other explanatory materials issued by the relevant commissioners.<sup>90</sup>

4.102 Consent is a concept that has developed differently in different legal contexts. There may be further developments that are of particular relevance to consent in connection with the use of surveillance devices, which could be hindered by restrictive legislative requirements. Further, a general statement of the requirements of consent may be insufficient to address each situation in which consent is relevant, but specific legislative requirements for consent in particular contexts are likely to be overly complex.<sup>91</sup>

4.103 Both express and implied consent are referred to in the definition of consent for practical reasons. In some circumstances, it may not be practicable to obtain express consent, for example, where an optical surveillance device is used in an area frequented by a large number of people. In that event, implied consent presents a practical and reasonable alternative.

4.104 One of the proposed new regulator's functions is to provide guidance about the operation of the legislation.<sup>92</sup> This could usefully include guidance about consent, including factors that might be relevant in determining whether effective consent has been given in particular circumstances. This is a practical and flexible approach that is specific to the context of the regulation of surveillance devices.<sup>93</sup>

### **Consent by vulnerable people**

4.105 With the exception of Western Australia, surveillance devices legislation in other jurisdictions does not include specific provisions about children or adults with impaired capacity. The legislation in Western Australia contains a limited exception,<sup>94</sup>

---

<sup>89</sup> See [4.108] ff below, in relation to children and adults with impaired capacity.

<sup>90</sup> See further [4.76] above.

<sup>91</sup> The ALRC reached a similar view in relation to consent under the *Privacy Act 1988* (Cth): See generally ALRC Report No 108 (2008), [19.61]–[19.65], Rec 19-1.

<sup>92</sup> See Rec 10-10(b), (d) below.

<sup>93</sup> The ALRC reached a similar view in relation to guidelines about consent under the *Privacy Act 1988* (Cth): see generally ALRC Report No 108 (2008) [19.16], [19.58]–[19.60], Rec 19-1, [22.70]. See also NSWLRC, *Privacy principles*, Report No 123 (August 2009) [2.98].

<sup>94</sup> See [5.289], [5.325] below. The legislation in Western Australia includes a specific exception for use of a listening device or an optical surveillance device by a person on behalf of a child or protected person under their care, supervision or authority who is a principal party to a private conversation or a private activity, 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: *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3).

but the circumstances in which that exception would apply could fall within the more general exceptions in the draft Bill.<sup>95</sup>

4.106 The draft Bill applies to all persons. As a result, it will apply to children and adults with impaired capacity. However, it does not include specific provisions dealing with a child or an adult with impaired capacity. The Commission recognises that some children and adults will not be able to give or refuse consent under the draft Bill, because they will not satisfy the requirement of capacity. In such a case, the general law governing consent, and the consent of children and adults with impaired capacity, will continue to apply.

4.107 The question of whether specific provisions might be required to address issues relating to capacity is properly a matter for consideration in the context of specific laws relevant to children and adults with impaired capacity, and is outside the scope of this review.

## Children

4.108 It is generally accepted that '[t]he principle of the law ... is that parental rights are derived from parental duty and exist only so long as they are needed for the protection of the person and property of the child'.<sup>96</sup> Parental rights gradually yield to a child's right to make their own decisions, as the child develops the ability to do so. Generally, whether a child is able to make a decision in particular circumstances depends upon whether the child has sufficient understanding, intelligence and maturity to fully comprehend the nature and consequences of the decision.<sup>97</sup>

4.109 In the context of information privacy, the OAIC and the OIC provide practical guidance about the consent of children. Their guidelines variously explain that, as far as possible, children should make their own decisions, and that there is no specific age at which a child may be presumed to have capacity, but 'as a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed'.<sup>98</sup> They also suggest that such assessments should be made on a case-by-case basis. Where a

<sup>95</sup> See, for example, exceptions to the use and communication or publication prohibitions that permit use that is reasonably necessary in the public interest or use that is connected with a serious threat: [5.283] ff, [6.92] ff, Recs 5-13, 5-15 and 6-5(c), (d).

<sup>96</sup> *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] 1 AC 112, 184.

<sup>97</sup> Ibid 182–9. This decision was endorsed by the High Court in *Secretary, Department of Health and Community Services v JWB and SMB ('Marion's Case')* (1992) 175 CLR 218, 237–8. These decisions, and other subsequent cases considering those decisions, are generally concerned with a child's capacity to consent to medical treatment.

See also OIC Guideline: Applications by and for children (2017) [4.2]; LexisNexis Australia, *Halsbury's Laws of Australia* (at 22 June 2015) 205 Family Law, 'Medical Treatment of Children' [205–2130].

See also the *Convention on the Rights of the Child*, GA Res 44/25, 20 November 1989, art 12(1), which states that where a child is capable of forming their own views, that child should have the right to express those views freely in relation to matters affecting them. The child's view should be 'given due weight in accordance with the age and maturity of the child'.

<sup>98</sup> OIC Guideline: Privacy for children (2012) 1; OAIC Guideline: Key concepts—Consent (2019). The OAIC guideline also states that, if it is impractical or unreasonable for the capacity of children to be tested on a case-by-case basis, then it may be presumed that children over the age of 15 have capacity to consent, unless there are indications otherwise. Children aged under 15 are presumed not to have capacity: [B.58]. The ALRC has expressed a similar view: ALRC Report No 108 (2008) [68.102]–[68.126], Recs 68–1 to 68–5.

child does not have capacity, there may be provision for a parent to consent or take some action on the child's behalf, but the child should remain involved and contribute to decisions to the extent that this is possible.<sup>99</sup>

4.110 The draft Bill does not include specific provisions about the capacity of a child to give or refuse consent. Legislation about this topic may be overly complex, and may not sufficiently take into account particular contextual circumstances.

4.111 Matters such as a child's capacity to give or refuse consent, including factors that are relevant to making an assessment of capacity, should be left to the operation of the general law. These are matters about which the proposed new regulator could provide guidance, in the context of the use of a surveillance device, or the communication or publication of surveillance information. Such guidance may be particularly useful for individuals, such as parents, who are assessing a child's capacity to consent.<sup>100</sup>

### **Adults with impaired capacity**

4.112 As explained previously, consent may be given or refused by an individual who has capacity, meaning generally that the individual can understand the nature and effect of their decision, form a reasoned view and communicate their decision.<sup>101</sup>

4.113 In Queensland, the term 'adult with impaired capacity' refers to a person over the age of 18 who is not capable of:<sup>102</sup>

- understanding the nature and effect of decisions about a particular matter;
- freely and voluntarily making decisions about that matter; and
- communicating their decisions in some way.

4.114 Where an adult has impaired capacity for a matter (for example, a decision about their finances, accommodation, employment or health care), another person may be appointed to make decisions about that matter on their behalf.<sup>103</sup> An

<sup>99</sup> OIC Guideline: Privacy for children (2012) 1; OIC Guideline: Key privacy concepts—agreement and consent (2013) [4.1]; OIC Guideline: Applications by and for children (2017) [1.0], [4.0], [4.2]; OIC, *Guidelines—Privacy Principles: Health agencies—Privacy, confidentiality, and children's information* (20 September 2019) <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/use-and-disclosure/health-agencies-use-or-disclosure-of-health-information>>; OAIC Guideline: Key concepts—Consent (2019) [B.56]–[B.57]; OAIC, *Children and young people* <<https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people/>>; OAIC, *Disclosing information about patients with impaired capacity* (2012).

In the context of health privacy, the child's 'maturity, degree of autonomy, understanding of the relevant issues and circumstances and the nature of the information being handled' are relevant considerations.

<sup>100</sup> In relation to Australian privacy law as it applies to children, the ALRC recommended that there should not be a test for capacity in legislation, but there should be guidance on matters such as assessments of capacity and seeking consent from a parent: ALRC Report No 108 (2008) [68.123], Rec 68-4; see also [70.52].

<sup>101</sup> See [4.76] above.

<sup>102</sup> *Guardianship and Administration Act 2000* (Qld) schs 2, 4 (definitions of 'capacity' and 'impaired capacity').

<sup>103</sup> This person might be appointed as the adult's attorney under an enduring document, or as the adult's guardian or administrator: see generally the *Powers of Attorney Act 1998* (Qld) and the *Guardianship and Administration Act 2000* (Qld). An 'enduring document' could be an enduring power of attorney or an advance health directive made under the *Powers of Attorney Act 1998* (Qld).



appointee may be given power to consent on behalf of an adult with impaired capacity to the use of a surveillance device, or the communication or publication of surveillance information, if it is connected to a matter for which they were appointed.

4.115 The draft Bill does not include specific provisions about the capacity of an adult to give or refuse consent. It may be useful for the new regulator to provide guidance about an adult's capacity to consent, including the assessment of an adult's capacity. In doing so, the new regulator might refer to the legislative scheme for the appointment of substitute decision-makers for adults with impaired capacity, and to explain the operation and application of that scheme.<sup>104</sup>

## RECOMMENDATIONS

### **Application of the Act**

- 4-1 The draft Bill should provide that the legislation binds all persons, including the State. The provision should also make it clear that the State cannot be prosecuted for an offence against the legislation.**

*[See Surveillance Devices Bill 2020 cl 3 and [4.2] above.]*

- 4-2 The draft Bill should not affect—**

- (a) the operation of the *Information Privacy Act 2009*; or**
- (b) the operation of another law regulating the use of surveillance devices.**

*[See Surveillance Devices Bill 2020 cl 4(a), (b) and [4.4] and [4.7] above.]*

### **Definition of 'surveillance device' and related definitions**

- 4-3 The draft Bill should define 'surveillance device' as:**

- (a) a listening device, an optical surveillance device, a tracking device, a data surveillance device; or**

In some circumstances, a person might be recognised as providing decision-making support to an adult with impaired capacity or acting as an adult's informal decision maker, without being formally appointed to any role. For example, an adult's family might help the adult to make decisions on an informal basis: see generally *Guardianship and Administration Act 2000* (Qld) ss 9(2)(a), 80U (definition of 'informal decision-maker'), 154(5), sch 4 (definition of 'support network'); *Disability Services Act 2006* (Qld) s 144 (definition of 'informal decision-maker').

<sup>104</sup>

This is consistent with the position of the ALRC and NZLC in relation to privacy law. Both concluded that legislation need not expressly recognise the authority of a decision-maker who is appointed by law, and that there should be guidelines developed to assist in the recognition and application of legislation about guardians and attorneys, and to provide information about supported decision-making. It was also concluded that legislation should not include special provision for people with impaired capacity who do not have a legally-authorised representative, with the ALRC explaining that this would involve an unacceptable level of risk of interference with an individual's privacy: ALRC Report No 108 (2008) [70.60]–[70.62], [70.84]–[70.85], Rec 70-3; NZLC, *Review of the Privacy Act 1993—Review of the Law of Privacy Stage 4*, Report No 123 (June 2011) [12.67]–[12.70], Rec 123.

- (b) a device that is a combination of any two or more of those devices.

*[See Surveillance Devices Bill 2020 cl 6 and [4.50]–[4.51] above.]*

- 4-4 The draft Bill should define ‘listening device’ as a device that is capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation. However, it should expressly exclude a hearing aid or a similar device used by an individual with impaired hearing.

*[See Surveillance Devices Bill 2020 cl 7 and [4.57]–[4.58] above.]*

- 4-5 The draft Bill should define ‘optical surveillance device’ as a device capable of being used to observe, monitor or visually record an activity. However, it should expressly exclude spectacles, contact lenses or a similar device used by an individual with impaired vision.

*[See Surveillance Devices Bill 2020 cl 8 and [4.59]–[4.60] above.]*

- 4-6 The draft Bill should define ‘tracking device’ as a device capable of being used to find, monitor or record the geographical location of an individual, vehicle or other thing.

*[See Surveillance Devices Bill 2020 cl 9 and [4.61] above.]*

- 4-7 The draft Bill should define ‘data surveillance device’ as a device or program capable of being used to access, monitor or record information that is input into, output from, or stored in a computer.

*[See Surveillance Devices Bill 2020 cl 10 and [4.63]–[4.64] above.]*

- 4-8 The draft Bill should define ‘computer’ as an electronic device for storing and processing information.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘computer’) and [4.63] above.]*

- 4-9 The draft Bill should define ‘surveillance information’ as information obtained, directly or indirectly, using a surveillance device.

*[See Surveillance Devices Bill 2020 cl 14 and [4.52] above.]*

- 4-10 The draft Bill should define ‘information’ to include:

- (a) a record in any form; and
- (b) a document.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘information’) and [4.52] above.]*

**Definition of consent**

**4-11 The draft Bill should define ‘consent’ as express or implied consent.**

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘consent’) and [4.100] above.]*



# Chapter 5

## Criminal prohibitions on the use of surveillance devices

INTRODUCTION .....	55
SURVEILLANCE DEVICES LEGISLATION .....	56
SUBMISSIONS.....	57
Prohibition on the use of a surveillance device for particular purposes.....	57
Criminal penalty.....	61
Exceptions to the prohibition on the use of a surveillance device .....	62
THE COMMISSION'S VIEW .....	78
The approach of the draft Bill .....	78
ELEMENTS OF THE USE PROHIBITIONS .....	79
Intention.....	79
Use, install or maintain surveillance devices .....	82
Prohibited uses.....	84
Private conversations and activities .....	86
Tracking devices and data surveillance devices .....	92
Parties .....	93
Consent .....	95
Criminal penalty.....	100
EXCEPTIONS TO THE USE PROHIBITIONS.....	101
Participant monitoring .....	102
Protection of lawful interests .....	103
Public interest.....	111
Safety and wellbeing .....	120
Location and retrieval of a lost or stolen vehicle or other thing.....	121
Authorised under another Act of the State or an Act of the Commonwealth .....	123
Prescribed circumstances .....	126
Security providers and insurance adjusters .....	127
Not for communication or publication to a person who is not a party .....	129
Lawful purpose.....	130
RECOMMENDATIONS .....	130

### INTRODUCTION

5.1 The terms of reference require the Commission to consider appropriate regulation of the use of surveillance devices, including listening devices, optical surveillance devices, tracking devices and data surveillance devices, and the use of emerging surveillance device technologies to ‘appropriately protect the privacy of individuals’. The Commission is also required to provide for offences relating to the unlawful use of surveillance devices.<sup>1</sup>

<sup>1</sup>

See terms of reference, paras 1, 3 in Appendix A.

5.2 In its Consultation Paper, the Commission sought submissions about the scope of a prohibition on the use of surveillance devices and appropriate exceptions to that prohibition, including whether and to what extent participant monitoring should be permitted.<sup>2</sup>

## SURVEILLANCE DEVICES LEGISLATION

5.3 Surveillance devices legislation is intended to protect privacy by limiting the use of surveillance devices to circumstances that are justified. In broad terms, such legislation prohibits the use (or the installation, maintenance or attachment) of surveillance devices for certain purposes (the ‘use prohibitions’) and is subject to particular exceptions.

5.4 In Queensland, the *Invasion of Privacy Act 1971* provides that:<sup>3</sup>

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 two years.

5.5 Similar provisions are included in surveillance devices legislation in other jurisdictions. In general, they provide that it is an offence for a person to use, install, maintain or attach one or more of the following devices:<sup>4</sup>

- 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’;<sup>5</sup>
- a tracking device to find, monitor or record the geographical location of a person or object; or
- a data surveillance device to access, track, monitor or record information that is input into, output from or stored in a computer.

5.6 Generally, it is not an offence for a person to use a surveillance device with consent, or in circumstances where an exception to the use prohibition applies.<sup>6</sup>

<sup>2</sup> QLRC Consultation Paper No 77 (2018) Q-6 to Q-14. As to participant monitoring, see [5.245] ff below.

<sup>3</sup> *Invasion of Privacy Act 1971* (Qld) s 43(1).

<sup>4</sup> *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). See also [2.27] ff above; QLRC Consultation Paper No 77 (2018) [2.70]–[2.74], [3.52]–[3.57].

<sup>5</sup> 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 in that Act.

<sup>6</sup> As to consent and the exceptions to the use prohibitions, see respectively [5.204] ff and [5.238] ff below.

## SUBMISSIONS

5.7 Most respondents were supportive of regulating surveillance, or the use of surveillance devices.<sup>7</sup>

5.8 Some respondents submitted that consideration could be given to adopting an approach similar to that taken in the surveillance devices legislation in other jurisdictions.<sup>8</sup> Other respondents submitted that the use of surveillance devices should be prohibited only in particular circumstances,<sup>9</sup> or that prohibitions should be limited and take into account the reasons for the use of the device.<sup>10</sup> In contrast, some other respondents submitted that the legislation should focus on the breach of the right to privacy,<sup>11</sup> or should regulate ‘surveillance’ rather than surveillance devices.<sup>12</sup>

### Prohibition on the use of a surveillance device for particular purposes

5.9 In the Consultation Paper, the Commission sought submissions about the purposes for which the use of a surveillance device should be prohibited. It also sought submissions about whether any prohibitions should be restricted to intentional or knowing use, be limited to private conversations and private activities, or extend to the attachment, installation and maintenance of a device.<sup>13</sup>

5.10 A number of respondents submitted that the use of a surveillance device should be prohibited for the purposes of:<sup>14</sup>

- listening to, overhearing, monitoring or recording a relevant conversation;
- observing, monitoring or recording visually a relevant activity;
- accessing, tracking, monitoring or recording information that is input into, output from or stored in a computer;
- determining the geographical location of a person, vehicle or object; and

<sup>7</sup> See also [3.28] ff above, as to alternative approaches to regulation.

<sup>8</sup> Eg, Submissions 8, 19. See also AAUS and Liberty Victoria Paper (2015) [4.1], [4.3], Recs 1, 3, adopted in Submission 39 from the AAUS, which advocated for the adoption of a nationally consistent surveillance devices regime. The AAUS also proposed that the term ‘surveillance device’ should be defined in a way that is technology neutral: see [4.37]–[4.41] above.

<sup>9</sup> Eg, Submission 10.

<sup>10</sup> Eg, Submissions 10, 37, 43.

<sup>11</sup> Eg, Submission 41, referring to the (then) Human Rights Bill 2019 (Qld) cl 25.

<sup>12</sup> Eg, Submissions 22, 25.

<sup>13</sup> QLRC Consultation Paper No 77 (2018) Q-6, Q-7, Q-14(d).

<sup>14</sup> Eg, Submissions 13, 18, 22, 40.

The AAUS suggested that a person should be prohibited from monitoring, observing, overhearing, listening to or recording a private activity (as explained at [5.20] below), or determining the geographical location of a person or object, without consent: AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

- some other purpose, such as the collection of biometric data.<sup>15</sup>

5.11 It was submitted that ‘any combination’ of these uses should be prohibited,<sup>16</sup> but that ‘overhearing’ a conversation that is not an intentional act should not be included.<sup>17</sup> A number of respondents submitted that the use of a surveillance device without consent should be prohibited.<sup>18</sup> Some respondents submitted that there could be some exceptions allowing for the use of a surveillance device in limited circumstances.<sup>19</sup>

5.12 The Brisbane City Council did not support ‘a total prohibition’ on use for any of the purposes listed above in respect of local government business, submitting that ‘an exception based approach would be more appropriate’. The Brisbane City Council uses technology, mainly overtly and with advanced notice, for a variety of purposes, such as surveillance of public places and recording the use of publicly available computers and internet services. This respondent submitted that ‘there is a need for appropriate surveillance options to be available to public asset owners and operators, to ensure fair and equitable access to, and proper management and protection of, public resources’.

5.13 An academic gave particular consideration to the regulation of optical surveillance devices. This respondent compared the ‘property-based approach’ (where a device cannot be used if it involves entry onto or into premises or a vehicle or interference with another thing without consent) with the ‘activity-based approach’ (where a device cannot be used to observe or record a ‘private activity’). This respondent observed that variations in legislation can lead to anomalous outcomes and submitted that an activity-based prohibition ‘may be more flexible and therefore offer greater protection for privacy interests’ than a property-based prohibition. It was also submitted that incorporating both approaches is unnecessary because an activity-based prohibition will sufficiently protect privacy interests.<sup>20</sup>

### ***Intentional or knowing use of a surveillance device***

5.14 A number of respondents submitted that the use prohibitions should be restricted to intentional or knowing use, or both.<sup>21</sup> It was submitted that the

<sup>15</sup> One respondent referred more specifically to the collection of ‘personal information, such as biometric data that is not required for, or relevant to,’ the particular purpose: Submission 10.

<sup>16</sup> Submission 13.

<sup>17</sup> Submission 15.

<sup>18</sup> Eg, Submissions 13, 18, 22, 33, 39.

<sup>19</sup> Eg, Submissions 13, 18, 19, 39. See also the discussion of submissions about possible exceptions at [5.31] ff below.

<sup>20</sup> Submission 19. See also the discussion of submissions about private conversations and private activities at [5.18] below.

<sup>21</sup> Eg, Submissions 13, 15, 18, 19, 22, 40. Several respondents submitted that the unintentional use of a device should not be an offence: Eg, Submissions 15, 18, 22.

Future Wise submitted that, if ‘surveillance’ is defined or understood to refer to ‘deliberate monitoring’ in order to obtain certain information, then ‘there is an element of intention, or knowing use of technology ... inherent in the prohibited conduct’.



prohibitions should ‘not capture accidental encroachments on privacy’,<sup>22</sup> or should focus on ‘deliberate monitoring’ and exclude ‘inadvertent actions’.<sup>23</sup> The AAUS suggested that there should be ‘a mental requirement of intent or recklessness to avoid capturing unintended or innocent surveillance’.<sup>24</sup>

5.15 A member of the public supported restricting the use prohibitions to intentional or knowing use, but cautioned that:<sup>25</sup>

careful consideration must be given in the proposed legislation to ensure [that] people who use [a] surveillance device [or] conduct surveillance activity do not rely on ‘unintentionality’ as an excuse to avoid responsibility for their actions or avoid regulation. (emphasis omitted)

5.16 QAI stated that intention should not be ‘a circumstance justifying a breach of privacy in circumstances where it is foreseeable that a breach might occur’ and that ‘[I]lack of intention, of itself, is not sufficient to excuse a violation of a person’s privacy’.

### ***Private conversations and activities***

5.17 Some respondents submitted that the use prohibitions should be restricted to private conversations and private activities.<sup>26</sup>

5.18 An academic noted that, in some jurisdictions, the definition of ‘private activity’ excludes an activity occurring outside a building or in a public place, submitting that this can lead to anomalous outcomes. It was submitted that ‘the question of whether there is a reasonable expectation of privacy ‘should simply be regarded as a question of fact depending on the ... circumstances’ and that ‘private activity’ should be defined without such exclusions’.<sup>27</sup>

5.19 In contrast, the Insurance Council of Australia supported a definition of ‘private activity’ that excludes an activity which occurs in or can be viewed from a public place. This respondent submitted that it is ‘essential’ for the insurance industry that permissible and prohibited surveillance is clearly defined, and that it is necessary to permit some surveillance activities in public places because that is where most insurance surveillance is undertaken.<sup>28</sup>

---

22 Submission 19.

23 Eg, Submissions 26, 35.

24 AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

25 Submission 13.

26 Eg, Submissions 13, 15.

27 Submission 19. This respondent submitted that the legislation should adopt a definition of ‘private activity’ in similar terms to the definition in the surveillance devices legislation in the Northern Territory and Western Australia. See also [5.13] above.

28 The Department of Agriculture and Fisheries also stated that the use of ‘visual surveillance devices’ should be permitted where the device is being used to record activities in public places that are not private acts, for example, a drone recording activity over waterways, CCTV cameras collecting data at boat ramps about how many people are fishing, or covert cameras in public locations to assist in investigations where there is a reasonable suspicion of a person committing an offence.

5.20 The AAUS suggested a use prohibition that involves ‘an understanding that each person holds a reasonable expectation of privacy with respect to certain activities and locations but not others’ and that is ‘restricted to instances where people have a reasonable expectation of privacy’. The AAUS considered that the terms ‘private conversation’ and ‘private activity’ are useful guides for determining reasonable expectations of privacy, but should be integrated into a broader concept of ‘private activity’ in the following terms:<sup>29</sup>

**Private activity** means any activity (including any communication) conducted in circumstances that may reasonably be taken to indicate that any or all of the parties to it expected it to be observed or overheard only by themselves, but does not include an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed or overheard by someone else.

5.21 Other respondents supported an approach based on expectations of, or intrusions into, privacy.<sup>30</sup> The QCCL stated that ‘privacy does not stop at the door of the house or the office’ and supported an approach based on ‘reasonable expectations of privacy’. The Department of Education submitted that one of the circumstances in which the use of a surveillance device should be prohibited is where the use is ‘an unreasonable intrusion into the private affairs of individuals using [a] public place’. A member of the public submitted that particular considerations should apply to the use of a surveillance device in private places, such as homes and yards, because people generally have a higher expectation of privacy in that context.<sup>31</sup>

5.22 An academic observed that individuals who enter public or quasi-public places (for example, respectively, a park or a shopping centre) respectively ‘maintain their right to privacy’, and have a reasonable expectation of ‘auditory privacy’ but not ‘visual privacy’. It was submitted that live visual surveillance does not infringe the right to privacy per se but that the further use of information that is obtained may do so, because:<sup>32</sup>

individuals reasonably expect to be observed while in public places, but they do not reasonably expect their actions to be recorded and stored, their movements from location to location to be tracked, or for their identities to be electronically matched with existing records.

5.23 Other respondents submitted that the use prohibitions should have a wider application.<sup>33</sup> For example, Future Wise submitted that the use prohibitions should

---

29 AAUS and Liberty Victoria Paper (2015) [4.3], Rec 4, adopted in Submission 39 from the AAUS.

30 Eg, Submissions 10, 39, 40.

31 Submission 13. Also, eg, Submission 5.

32 Submission 17. This respondent submitted that the use of a surveillance device should occur only where particular justifications outweigh the right to privacy, and that notification about surveillance ‘may be a necessary precondition to help minimise the intrusion of surveillance already justified on other grounds, but cannot be considered a justification in and of itself’.

33 Eg, Submissions 18, 25.

In the context of the use of a surveillance device in the public interest, Animal Liberation Queensland submitted that the legislation should clearly distinguish between private activities and commercial activities involving vulnerable animals, and that the legislation should ‘reflect the intent of the surveillance rather than just whether or not a surveillance device was used’.

‘extend to all activities, based on the principle that free, prior, and informed consent should be required before collecting data or recording activities’. The prohibitions would therefore apply to private conversations and activities, and activities occurring in public forums, such as conference presentations.

5.24 QAI submitted that ‘[t]he content of [a conversation] should be the determining factor as to whether use of a surveillance device is prohibited in a particular situation’. This respondent gave the example of a conversation between two colleagues about the support of a person with disability, observing that this may not be a ‘private conversation’ if it occurs in a workplace but that it may contain private information that should not be permitted to be disclosed.

### ***Attachment, installation and maintenance of a surveillance device***

5.25 A number of respondents supported the extension of the use prohibitions to the attachment, installation or maintenance of a surveillance device.<sup>34</sup> One respondent submitted that ‘careful consideration’ should be given to the ‘augmentation’ of surveillance devices by, for example, mounting a device onto a structure and thereby impacting on the privacy of another person.<sup>35</sup>

5.26 The QCCL stated that the legislation ‘should provide the broadest level of protection’. This respondent observed that the actions of attaching, installing or maintaining a device are necessary for the device to be used and that the extent to which they are seen as involving a lower level of culpability can be reflected in a lesser penalty.

5.27 Future Wise expressed concern about the potential breadth and difficulty of enforcing the use prohibitions, in part because of the range of current technologies that could be used as a surveillance device.

### **Criminal penalty**

5.28 In the Consultation Paper, the Commission sought submissions on whether a contravention of a use prohibition should be punishable as a criminal offence, or by a civil penalty as alternatives.<sup>36</sup>

5.29 Most respondents submitted that a contravention of a use prohibition (or a communication or publication prohibition) should be punishable as criminal

<sup>34</sup> Eg, Submissions 13, 15, 18, 40. The AAUS suggested that a person should be prohibited from installing or using a surveillance device, and from causing a surveillance device to be installed or used: AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

One other respondent suggested that use prohibitions should ‘extend to the development of technologies and be adapted in accordance with the progress of the technology’: Submission 33.

<sup>35</sup> Submission 13. It was also observed that this would enhance the ‘visual capture reach’ of a relevant device.

<sup>36</sup> QLRC Consultation Paper No 77 (2018) Q-21. This question related to both the use prohibitions and the communication or publication prohibitions.

offences.<sup>37</sup> A number of those respondents submitted that civil penalties could also be available as an alternative to the criminal penalty.<sup>38</sup>

5.30 Some respondents commented that the existing criminal penalties are insufficient and should be increased.<sup>39</sup> In contrast, the QCCL submitted that criminal penalties should not exceed a period of 12 months of imprisonment. The OIC observed generally that the penalties should ‘reflect the seriousness of the breach, [and] the gravity of the act or intrusion into an individual’s privacy’.

### **Exceptions to the prohibition on the use of a surveillance device**

5.31 In the Consultation Paper, the Commission sought submissions on the exceptions that should apply in relation to any prohibitions on the use of a surveillance device. In particular, the Commission sought views about the use of a surveillance device with consent, the extent to which participant monitoring should be permitted, and whether there should be other exceptions that apply in particular circumstances.<sup>40</sup>

5.32 QAI submitted that exceptions to the use prohibitions must be given careful consideration because they will impact on privacy:<sup>41</sup>

In all circumstances, the focus must be on balancing the right to privacy with competing human rights, such as the right to protection from violence, abuse and neglect and also considering the flow on effects of any potential breach of privacy.

In circumstances where surveillance is justifiable, ongoing safeguards must be implemented to ensure that the surveillance, and the information obtained via surveillance, is limited to the extent necessary to achieve the purpose.

5.33 DTMR submitted that ‘broad’ prohibitions on the use of surveillance could have ‘unintended implications’, and that accordingly, exceptions are required.

### ***Use of a surveillance device with consent***

5.34 A number of respondents made submissions about the use of a surveillance device with consent.<sup>42</sup>

---

<sup>37</sup> Eg, Submissions 13, 18, 19, 22, 25, 33, 40, 41, 43.

<sup>38</sup> Eg, Submissions 18, 22, 25, 33, 40, 41, 43. The AAUS suggested that civil penalties should attach to the use prohibitions with criminal penalties reserved as an alternative for its more serious proposed offence involving intimidation, harassment or harm: AAUS and Liberty Victoria Paper (2015) [4.3], [4.5], Recs 3, 7, adopted in Submission 39 from the AAUS. The QLS commented that, while civil penalties may be appropriate for wrongful behaviour which would not otherwise meet the ‘standard’ required for police prosecution, the ‘lower standard of proof requires serious consideration of associated penalties’ and the availability of appropriate reviews of regulatory decisions. Civil penalties are imposed by civil rather than criminal court processes and are usually in the form of monetary penalties (fines): see QLRC Consultation Paper No 77 (2018) [3.223]–[3.230].

<sup>39</sup> Eg, Submissions 3, 12, 13. A few respondents noted that the criminal penalties should be sufficient to act as a deterrent: eg, Submissions 13, 38.

<sup>40</sup> QLRC Consultation Paper No 77 (2018) Q-8 to Q-14.

<sup>41</sup> Submission 33.

<sup>42</sup> As to the general concept of consent, including its meaning and scope, see [4.75] ff above.

5.35 Some respondents made submissions to the effect that if consent is given, then a person should be permitted to use a surveillance device or more generally to engage in surveillance.<sup>43</sup> The Department of Education submitted that '[i]f valid consent is given, then surveillance may be used in any reasonable circumstances'. The Brisbane City Council stated that 'in circumstances where the surveillance is appropriate and proportionate, surveillance devices should be able to be used with consent'. Similarly, the OIC submitted that 'as a general principle, surveillance should ordinarily be permitted if it occurs with consent'.

5.36 In particular, some respondents submitted that the use of a surveillance device should not be prohibited where there is consent to its use. It was suggested in relation to the use prohibitions that a lack of consent could operate as an element, or alternatively, the provision of consent could operate as an exception.<sup>44</sup> The Townsville Community Legal Service Inc. observed that '[g]iven Queensland's current position, use by actual informed consent only would be a significant change'.<sup>45</sup>

5.37 A number of respondents made submissions about consent in a particular context, or in connection with a particular device. Generally, respondents submitted that consent should be obtained from each of the parties to the conversation or activity.<sup>46</sup> The AAUS submitted that consent should also be obtained from the following persons:<sup>47</sup>

- for use of a surveillance device to determine the location of a person, that person;<sup>48</sup>
- for use of a surveillance device to determine the location of an object, the person in lawful possession or having lawful control of that object.<sup>49</sup>

5.38 In response to the current legislation, a member of the public submitted that '[a]ny recording [of a conversation] should require permission of all parties or each party should be made aware of the recording and have the option for it to be terminated'.<sup>50</sup> Another member of the public submitted that a person should be

<sup>43</sup> Eg, Submissions 10, 22, 25, 35, 38.

<sup>44</sup> See [5.11] above and eg, Submissions 13, 15, 18, 19, 22, 33, 39, 40, 41.

<sup>45</sup> Submission 41. Currently, the *Invasion of Privacy Act 1971* (Qld) s 43(2)(a) provides that it is not an offence for a person to use a listening device to record a private conversation without consent, where that person is a party to the conversation: see [5.245] ff below.

<sup>46</sup> Eg, Submissions 13, 19, 22, 33, 39. QAI, whose submission focussed on people with disability, submitted that recording a person should generally be done with the person's consent, including their consent to the purpose of the recording and with the opportunity to view and comment on the recording.

<sup>47</sup> AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

<sup>48</sup> QAI also submitted that tracking of a person should generally be done with the person's consent. This respondent suggested that, if the tracking device cannot be used with the person's consent, the purpose of the device should be explained to the person and the person given an opportunity to view the device and the information recorded by it.

<sup>49</sup> This respondent clarified that this should not apply where the use is for the sole purpose of retrieval of that object to its owner: AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS, and see [5.98] below.

<sup>50</sup> Submission 22.

permitted to use a surveillance device only with the consent of each direct or indirect subject of the surveillance, and should not be permitted to use a device if consent is expressly refused or withdrawn.<sup>51</sup>

5.39 Some respondents suggested varying the requirements for consent, for example, by requiring written consent where there is 'greater risk' to privacy, or by providing that a listening device or an optical surveillance device may be used if a person has indicated that they are recording, but requiring written consent for the use of a tracking device or a data surveillance device.<sup>52</sup> The Brisbane City Council stated that consent requirements will depend on the technology being utilised and on practicalities, for example, signage might be appropriate for the optical surveillance of public places, and acknowledgement of terms and conditions might be suitable for computer-based surveillance.

### ***A general exception for use of a surveillance device for participant monitoring***

5.40 The Commission sought submissions on whether a party to a conversation or activity should be permitted to use a surveillance device to monitor or record the conversation or activity without the consent of the other parties to that conversation or activity.<sup>53</sup>

5.41 The Commission also sought submissions on whether, as an alternative to a general exception, there should be exceptions that would permit participant monitoring in particular circumstances, and whether those exceptions should also apply in circumstances that do not involve participant monitoring.<sup>54</sup>

5.42 A few respondents expressed support for a general exception to the use prohibitions that would permit participant monitoring.<sup>55</sup> DTMR preferred a general exception, but submitted, alternatively, that consideration be given to specific exceptions that would allow agencies to use a surveillance device to perform official duties or deliver safety services.<sup>56</sup>

5.43 A member of the public stated that participant monitoring should be permitted where a conversation is with a business, organisation or government

---

51 Submission 13.

52 Eg, Submissions 13, 15.

53 QLRC Consultation Paper No 77 (2018) Q-9.

54 Ibid Q-10 to Q-13.

55 Eg, Submissions 2, 36. Another respondent observed that, if participant monitoring is maintained, 'greater clarity' about the circumstances in which participant monitoring is permitted and 'the evidentiary context' of such monitoring should be considered: Submission 41.

56 DTMR gave as an example the use of body-worn cameras by employees who are working independently in a remote area or on public transport. This respondent indicated that it 'supports the need for clear rules around usage, with appropriate monitoring and reporting'.

The Department of Agriculture and Fisheries submitted that participant monitoring should not be prohibited for law enforcement purposes, but if it were, specific exceptions for use in a person's lawful interests, in the public interest, for a person's safety and wellbeing or where it is not for communication or publication to a non-party should be included. This respondent also suggested an additional exception; namely, if the participant monitoring is 'likely to result in the provision of evidence in legal proceedings'.

department, but should not be permitted where a conversation is with an individual who is not at work.<sup>57</sup>

5.44 Most respondents who addressed this issue opposed a general exception that would permit participant monitoring.<sup>58</sup> A member of the public stated that such an exception 'is inconsistent with the general expectation that monitoring will not occur without appropriate consent',<sup>59</sup> and others were opposed because the monitoring of a conversation or activity should occur only with permission or consent.<sup>60</sup>

5.45 The OIC agreed with the Commission's preliminary view that legislation should not include a general exception for participant monitoring, noting that this approach is consistent with surveillance devices legislation in a number of other jurisdictions, the Commonwealth legislation regulating telecommunications and the position taken in other reviews and inquiries that have considered the issue.

5.46 The OIC stated that a prohibition on participant monitoring would 'modernise Queensland's surveillance legislation to respond to increased capability of individuals to engage in surveillance due to advances in technology'. A member of the public expressed a similar view noting, in particular, that there is now greater scope for covert recording.<sup>61</sup>

5.47 The Toowoomba Regional Council observed that, if participant monitoring were generally permitted, the person conducting the monitoring would have 'the benefit of knowing' about the use of a device and could 'choose their behaviour accordingly', but other participants would not have that benefit.<sup>62</sup>

5.48 Future Wise opposed a general exception to permit participant monitoring on the basis that other, more specific exceptions will 'provide sufficiently for circumstances of covert participant monitoring' and that, except for those specific circumstances, there is no need to use a surveillance device without consent.

5.49 The QCCL observed that there are 'strong competing considerations' on this issue. Relevantly, participant monitoring is a common means of 'self-protection', there is always a risk of a conversation being recorded in some way (such as note-taking), and regulating only one means of monitoring a conversation introduces a level of inconsistency. However, this respondent also stated:

---

57 Submission 2.

58 Eg, Submissions 10, 13, 18, 22, 25, 33, 38, 40. One respondent stated that the types of surveillance that are prohibited should be based upon purpose, relevance, location and the types of personal information that can be collected: Submission 10.

59 Submission 13. This respondent also stated that '[p]eople engaged in personal or civil conversations and activities generally expect a higher level of transparency of behaviour and respect for privacy in these situations'. The OIC made a similar submission, noting the view in VLRC Report No 18 [6.75] that, 'as a rule, a person should be able to conduct private conversations and engage in private activities without those events being recorded without their consent'.

60 Eg, Submissions 22, 33.

61 Submission 13.

62 Submission 18.

To some extent, these arguments reflect the view of the world developed before the development of the digital world. Modern digital devices have a capacity to record and distribute information which dwarfs the capacity of people to make and distribute written notes of conversations.

Development of modern information technology, has put information privacy at the front and centre of peoples' concerns. It is a clear breach of the [principles of] information privacy that a person should be able to record another [person's] conversation, without their consent. Note taking, like the tourist taking a photograph in the mall, is an activity which can be seen. The covert recordings of a conversation by a participant in it, is in our view no more different from the covert recording of the conversation by a third party.

5.50 The QCCL concluded that situations where a person may need to record a conversation to protect their interests can be addressed by 'appropriately drafted exceptions', and that this 'will put the focus on the interests which the recording of the conversation is designed to serve and not on the simple fact that the participant has recorded it'.<sup>63</sup>

***Use of a surveillance device for participant monitoring in specific circumstances***

5.51 Many of the respondents who opposed a general exception for participant monitoring supported specific exceptions that would permit participant monitoring in particular circumstances. Various, respondents referred to circumstances where the use is in a person's lawful interests, in the public interest, or consistent with a person's safety or wellbeing.<sup>64</sup>

5.52 The Brisbane City Council expressed support for participant monitoring in those particular circumstances because it may sometimes be 'necessary for [the] Council to conduct its business', including in relation to 'matters of public safety, self-harm management, emergency situations and enforcement matters'. DTMR, while supporting those circumstances as 'sound examples of suitable exceptions to a general prohibition', stated that '[e]xceptions that permit participant monitoring in particular circumstances need to be considered on a case by case basis depending on need and intent'.

5.53 The OIC indicated that these circumstances might be relevant exceptions to a general prohibition on participant monitoring. The OIC also observed that '[i]dentifying the *particular* circumstances for any exceptions to a general prohibition on participant monitoring is complex and subject to divergent views', and that '[b]alancing the privacy rights of individuals with other legitimate rights and interests, such as public interest considerations, presents a number of challenges'.<sup>65</sup> The OIC stated that it did not support 'overly broad exceptions'<sup>66</sup> and that:

---

<sup>63</sup> Submission 40. The QCCL also suggested that this should be conditional upon the introduction of a tort for serious invasions of privacy.

<sup>64</sup> Eg, Submissions 10, 13, 18, 25, 35, 38. See also the Department of Agriculture and Fisheries at n 56 above.

<sup>65</sup> Emphasis in original.

<sup>66</sup> Noting the views of the ALRC and VLRC, discussed in QLRC Consultation Paper No 77 (2018) at, eg, [3.95], [3.118], [3.128], [3.133].



whether the surveillance activity is justified will depend on the context and circumstances of each particular case. Each case will require the balancing of competing rights and interests to determine if the incursion into an individual's privacy was necessary and proportionate to the protection of the relevant interest.

5.54 Some of these respondents also expressed support for the operation of similar exceptions outside of participant monitoring, for example, where a person who is not a party uses a surveillance device to protect a lawful interest, in the public interest, or because it is consistent with another person's safety and wellbeing.<sup>67</sup> One respondent observed that this 'provides a balanced approach' and that these 'are confined to limited and exceptional circumstances and the benefits under these circumstances would generally outweigh any costs [or] risks to privacy', but subject to the caveat that use should not be permitted where consent has been expressly refused or withdrawn.<sup>68</sup>

5.55 Other respondents generally considered that the monitoring of a conversation or activity should occur only with consent, although it was observed that there might appropriately be an exception in circumstances where there is violence.<sup>69</sup> One respondent stated, in this context, that '[g]iven the importance of privacy as a fundamental human right, and the difficulties in balancing competing rights, the threshold for an exemption to this right must be high'.<sup>70</sup>

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

5.56 A number of respondents submitted that there should be an exception permitting the use of a surveillance device to protect a person's lawful interests. There was support for this to operate as a specific exception permitting participant monitoring in those circumstances,<sup>71</sup> and more generally as a circumstance in which a person is permitted to use a device without consent.<sup>72</sup>

5.57 In relation to participant monitoring, the OIC submitted that an exception 'might include circumstances where it is reasonably necessary to protect a person's lawful interest', but did not support an 'overly broad' exception. In particular, the OIC

<sup>67</sup> Eg, in relation to some or all of those exceptions, Submissions 10, 13, 19, 25, 35. One respondent stated that the exceptions that apply in relation to participant monitoring should also apply in other circumstances: Submission 25.

<sup>68</sup> Submission 13.

<sup>69</sup> Eg, Submissions 22, 33. For example, one respondent suggested there could be an exception where there is a real and imminent threat of violence. This respondent also observed that there might need to be some alternative means of approval for people who cannot consent, for example, a person with a disability: Submission 22.

<sup>70</sup> Submission 33. The Townsville Community Legal Service Inc. also commented that some private matters now fall within the realm of public interest (for example, domestic violence and elder abuse), but that an absence of consent must still be balanced against other rights.

<sup>71</sup> Eg, Submissions 10, 13, 18, 35, 36, 38, 40. See also Department of Agriculture and Fisheries, in n 56 above.

<sup>72</sup> Eg, Submissions 10, 13, 15, 18, 19, 35, 40.

noted that an exception should not be excessively broad or narrow, and should not obviate the primary purpose of protecting privacy.<sup>73</sup>

5.58 The Department of Education submitted that an exception should permit participant monitoring where it is ‘undertaken or performed to protect a person’s legitimate or lawful interests’.

5.59 An academic submitted that there may be ‘a need for a more general exception where ... the surveillance is no more than is necessary to protect a person’s lawful interests’. For example, this could apply to homeowners conducting indoor or outdoor surveillance for security purposes, but would not extend to a homeowner installing cameras to observe or record the intimate activities of guests.<sup>74</sup>

5.60 The QCCL submitted that an exception permitting use to protect a person’s lawful interests ‘should apply to all devices’.<sup>75</sup>

5.61 A few respondents submitted that legislation should not include an exception permitting the use of a surveillance device to protect a person’s lawful interests.<sup>76</sup> Future Wise submitted that ‘there is no need for covert surveillance’ in these circumstances.

### ***The meaning or scope of ‘lawful interests’***

5.62 Some respondents submitted that the scope of this exception, or the meaning of the term ‘lawful interests’, needs to be clear.<sup>77</sup>

5.63 Some respondents considered the application of the term ‘lawful interests’ in a legal context. A government department submitted that it should incorporate use of a device in the course of investigating offences and use that is permitted or required by another law.<sup>78</sup> The Insurance Council of Australia submitted that the term should include contractual rights and the defence of an insurance claim by an insurer, and should be broad enough to apply to corporations.<sup>79</sup> The Women’s Legal Service Qld submitted that careful definition is required to avoid a perpetrator of domestic violence claiming that it is in their ‘lawful interests’ to conduct surveillance of their former partner and children to inform family law proceedings.

---

<sup>73</sup> Noting the comments of the VLRC and the New South Wales Court of Criminal Appeal in *Sepulveda v The Queen* (2006) 167 A Crim R 108, 134 [115], [142], discussed in QLRC Consultation Paper No 77 (2018) [3.114], [3.118].

<sup>74</sup> Submission 19.

<sup>75</sup> In other jurisdictions, this exception applies in relation to listening devices and optical surveillance devices: see generally QLRC Consultation Paper No 77 (2018) [3.63] and [3.106] ff.

<sup>76</sup> Eg, Submissions 22, 25.

<sup>77</sup> Eg, Submissions 15, 27.

<sup>78</sup> Submission 15.

<sup>79</sup> This respondent observed, in relation to contractual rights and defence of claims, that the APPs contain ‘clear exemptions’. This respondent also submitted that the term ‘lawful interests’ ‘should be given its natural interpretation’.

5.64 In contrast, the QCCL stated that ‘the decisions of the courts on the existing provision [for lawful interests] provide an approach that adequately identifies circumstances in which a person’s specific interests override the other person’s privacy claims’.<sup>80</sup> Similarly, an academic observed (in relation to a similar exception for communication or publication to protect a lawful interest) that ‘[t]here is advantage in this being a general exception, to be determined on the facts of the individual case’.<sup>81</sup>

### ***Use of a surveillance device in the public interest***

5.65 A number of respondents submitted that there should be an exception permitting the use of a surveillance device where it is in the public interest. There was support for this to operate as a specific exception permitting participant monitoring in those circumstances,<sup>82</sup> and more generally as a circumstance in which a person is permitted to use a device without consent.<sup>83</sup>

5.66 One respondent commented that the term ‘public interest’ could be open to interpretation, for example, the media’s interpretation would be different from an individual’s interpretation.<sup>84</sup>

5.67 Other respondents made submissions about matters that should be encompassed by an exception permitting use of a surveillance device in the ‘public interest’. For example, it was suggested that the exception should apply to the exposure of corruption or systemic problems in government agencies or departments,<sup>85</sup> bringing to light actions that are illegal or unacceptable to the public;<sup>86</sup> or to the protection of assets and enforcement.<sup>87</sup> The Department of Environment and Science stated that:

The department sees benefit in permitting the use of a surveillance device by government employees, contractors and emergency service volunteers in circumstances involving the public interest for proper administration of government including site management, public health and safety and critical incidents and emergency situations (for example, bushfire control, natural disasters and search and rescue), without it being an offence. However, this should be balanced against the reasonable expectation of individual privacy, be proportionate to the purpose and include regulation around secure storage of information. Reasonable consistency with other jurisdictions should also be considered.

---

<sup>80</sup> Also, eg, Submission 26, at [5.63] and n 79 above.

<sup>81</sup> Submission 19.

<sup>82</sup> Eg, Submissions 10, 13, 18, 25, 35, 36, 38. One respondent also described an exception for ‘public safety and security’: Submission 18. See also Department of Agriculture and Fisheries at n 56 above.

<sup>83</sup> Eg, Submissions 10, 13, 15, 18, 19, 25, 35, 39.

<sup>84</sup> Submission 18. One respondent observed that the term ‘public interest’ is not defined in the legislation in other jurisdictions and relies on judicial interpretation: Submission 14. Another respondent similarly observed that a ‘public interest’ exception may be broad and may need definition: Submission 27.

<sup>85</sup> Eg, Submission 27.

<sup>86</sup> Submission 37, in the context of animal welfare.

<sup>87</sup> Submission 35.

5.68 An academic suggested an alternative, more clearly prescribed approach to a public interest exception, observing that a broad exception ‘may be open to subjectivity and potential abuse’. This respondent submitted that the ALRC’s suggestion for a defence of ‘responsible journalism’<sup>88</sup> could be adapted into a broader exception applying where:<sup>89</sup>

- (a) the surveillance was carried out for the purposes of investigating matters of significant public concern;
- (b) the person conducting the surveillance reasonably believed that conducting the surveillance was in the public interest; and
- (c) the surveillance was necessary and appropriate for achieving that public interest, and the public interest could not have been satisfied through other reasonable means.

5.69 It was submitted that an exception of this nature could apply, for example, to use of a surveillance device relevant to journalism, recording of environmental damage, or recording of a criminal offence to provide information to law enforcement.

5.70 A few respondents submitted that the legislation should not include an exception permitting the use of a device in the public interest.<sup>90</sup> The QCCL stated that, in general terms, they did not support public interests exceptions, observing that the term public interest is ‘inherently vague’ and that historically this kind of exception tends to be ‘under inclusive’. However, this respondent did express support for ‘the public interest in a free media’ and a specific exception for responsible journalism.<sup>91</sup>

### ***Use of a surveillance device for safety and wellbeing***

5.71 A number of respondents submitted that there should be an exception permitting the use of a surveillance device where it is consistent with a person’s safety or wellbeing. There was support for this to operate as a specific exception permitting participant monitoring in those circumstances,<sup>92</sup> and more generally as a circumstance in which a person is permitted to use a device without consent.<sup>93</sup>

5.72 Respondents variously submitted that an exception of this type could apply:

- when the use of a device is consistent with, or for the protection of, the safety and wellbeing of the user or another person; it is related to matters of security,

---

<sup>88</sup> See ALRC Report No 123 (2014) [14.58] ff; see also QLRC Consultation Paper No 77 (2018) [3.133]–[3.134].

<sup>89</sup> Submission 19. It was submitted that this exception would accommodate, but would not be limited to, instances of responsible journalism, and that it should be complemented by examples, including specific reference to journalism.

<sup>90</sup> Eg, Submissions 22, 40.

<sup>91</sup> Submission 40. As to an exception relevant to the media, see [5.91] ff below, and particularly [5.94]. The QLS also expressed support for an exception in relation to responsible journalism: Submission 43, and see [5.95] below.

<sup>92</sup> Eg, Submissions 10, 13, 18, 25, 35, 36, 38. See also Department of Agriculture and Fisheries at n 56 above.

<sup>93</sup> Eg, Submissions 10, 13, 15, 18, 19, 25, 32, 35, 39.

personal safety or emergency, or it is ‘reasonably necessary to protect a person from significant harm’;<sup>94</sup> or

- to protect a person from ‘imminent threat of serious injury or death’ and property from ‘imminent threat of substantial damage’.<sup>95</sup>

5.73 QAI and a member of the public submitted that a surveillance device should not ordinarily be used without consent, but observed that it might be appropriate in situations involving ‘violence, abuse or coercion’ or a real and ‘imminent threat of violence’.<sup>96</sup> In relation to people with disability, QAI submitted generally that the rationale for monitoring must primarily be to safeguard a person with disability from risk, whilst being the least restrictive or intrusive option and not impacting on their right to privacy and dignity.

5.74 The QCCL submitted that health and safety exceptions ‘are open to abuse’. This respondent submitted that if there were an exception on this ground, it should be similar to the approach taken in Tasmania. Specifically, it should be required that there is an ‘imminent threat of serious violence or substantial property damage’ and that it is necessary to use the device immediately.<sup>97</sup>

### ***Use of a surveillance device that is not for communication or publication***

5.75 Most respondents who considered this issue did not support an exception for participant monitoring if the recording party does not intend to communicate or publish the conversation or activity (or a report of it) to a non-party.<sup>98</sup>

5.76 A number of respondents observed, consistently with the VLRC, that recordings ‘may fall into the hands of third parties’.<sup>99</sup> The OIC submitted that:

This risk is exacerbated by the increasing availability of surveillance devices allowing information to be disseminated rapidly and with relative ease. When combined with the other known risks, such as the potential for unintentional or unauthorised access to this information, it is likely to result in undue interference with privacy.

<sup>94</sup> Eg, Submissions 10, 25, 35, 39. One respondent also submitted more particularly that a person should be permitted to record information about others in circumstances involving a potential threat or to protect their safety, including where they are recording an interaction with security personnel or police, and that such recordings should not be able to be seized or deleted: Submission 25.

<sup>95</sup> Submission 19.

<sup>96</sup> Submissions 22, 33. More specifically, QAI submitted that where there is a reasonable concern of violence, abuse or coercion but the offender is unknown, monitoring without consent to obtain admissible evidence might be justified.

<sup>97</sup> See also *Listening Devices Act 1991* (Tas) s 5(2)(c)(i). The QCCL also suggested that a ‘health and safety’ exception is not necessary considering the decision in *Thomas v Nash* (2010) 107 SASR 309, discussed in QLRC Consultation Paper No 77 (2018) [3.112].

<sup>98</sup> Eg, Submissions 13, 18, 22, 25, 38, 40. A government department stated that an exception of this kind of support the inclusion of this type of exception, stating that it ‘could be construed as inhibiting or preventing the use of collected material ... for further investigation and internal reporting’: Submission 36.

Conversely, another government department expressed support for this exception. It stated that participant monitoring should not be prohibited for law enforcement purposes but, if it were, then this exception should be included: Submission 15; see also n 56 above.

<sup>99</sup> Eg, Submissions 13, 38, 40.

### ***Use of a surveillance device in other exceptional circumstances***

5.77 In the Consultation Paper, the Commission sought submissions about whether there were other circumstances in which the use of a surveillance device should be permitted or should not be an offence. Examples given were when the use of a device is: for a lawful purpose; in the course of a person's occupation; to locate or retrieve a device; unintentional; or in other prescribed circumstances.<sup>100</sup>

### ***Use of a surveillance device for a lawful purpose***

5.78 A number of respondents submitted that the use of a surveillance device should be permitted, or should not be an offence, where it is for a lawful purpose.<sup>101</sup> One respondent submitted that a 'lawful purpose should include where the surveillance is permitted by another law'.<sup>102</sup>

5.79 The QCCL submitted that it did not support an exception of this kind 'on the basis that it is too vague and open to abuse'.

5.80 QAI submitted that, where surveillance is for a lawful purpose, it 'must be recognised that it is still a breach of ... privacy' and that 'competing rights must be carefully balanced'.

### ***Use of a surveillance device by particular occupations***

5.81 The Commission sought submissions about whether the use of a surveillance device should be permitted, or should not be an offence, for certain people acting in the course of their occupation, such as media organisations, journalists, private investigators and loss adjusters.<sup>103</sup>

5.82 Most respondents who addressed this question supported some provision for the use of a surveillance device by those occupations.<sup>104</sup> The Brisbane City Council commented that, '[w]here specific occupations require surveillance activities as part of their role, these may be considered under other legislation specific to those activities'.

### ***Private investigators and loss adjusters***

5.83 In information provided to the Commission, the Institute of Mercantile Agents Limited explained that surveillance devices might be used by private investigators to gather video or photographic evidence, commonly in relation to

---

<sup>100</sup> QLRC Consultation Paper No 77 (2018) Q-14.

<sup>101</sup> Eg, Submissions 13, 15, 18, 43.

One respondent expressed some support for this exception, but stated that it depended upon the particular purpose and whether there was any 'gatekeeper': Submission 22.

<sup>102</sup> Submission 15. This respondent gave as an example that the *Fisheries Act 1994* (Qld) requires some commercial fishers to install and use vessel tracking units on their boats.

<sup>103</sup> QLRC Consultation Paper No 77 (2018) Q-14(b).

<sup>104</sup> Eg, Submissions 13, 15, 18, 19, 40. A member of the public submitted that there should not be any circumstances in which the use of a device is permitted, or is not an offence, for those occupations: Submission 2.

(among other things) insurance fraud, property theft or monitoring of a person's movements for other legitimate reasons for clients, which are primarily insurers and law firms.<sup>105</sup>

5.84 A number of respondents submitted that the use of a surveillance device by a private investigator or a loss adjuster acting in the course of their occupation should be permitted, or should not be an offence.<sup>106</sup>

5.85 Future Wise submitted that, '[as] a general principle, civil surveillance should not be undertaken covertly, but that surveillance by private investigators or loss adjusters 'represent[s] a justifiable exception'. However, that surveillance should 'only be undertaken by registered investigators subjected to oversight as to qualifications, conduct, data storage, disclosure and with sanctions for [a] breach'. This respondent supported an exception for use that is in the public interest.

5.86 An academic submitted that the legislation should provide certainty to licensed private investigators, loss adjusters and licensed security providers, who may use surveillance in their usual operations. It was submitted that those occupations might sometimes rely on an exception for use in the public interest, but that surveillance in a person's private interests should be the subject of a specific, limited exception. The exception should permit the use of a surveillance device by persons in those or other occupations where the use is 'part of their normal operations' and 'reasonably necessary to protect a person's lawful interests'.<sup>107</sup>

5.87 The Insurance Council of Australia and the QCCL addressed the use of surveillance by insurers and insurance adjusters. Both submitted that use should be permitted in connection with the assessment and investigation of insurance claims, in order to detect fraud and avoid delayed claims assessments and increased premiums.

5.88 The QCCL endorsed the recommendation of the NSWLRC that insurers should be authorised to conduct covert surveillance and to contract that work out to private investigators.<sup>108</sup> It was also submitted that a relevant code of conduct should be formulated, and that there should be audits and enforceable remedies for invasions of privacy.

5.89 The Insurance Council of Australia observed that there needs to be a regulatory framework that 'provides clear rules for legitimate surveillance activities', including about surveillance in public places. This respondent, noting that in

---

<sup>105</sup> Information provided to the QLRC by the Institute of Mercantile Agents Limited, 2 July 2019. The NSWLRC stated that 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].

<sup>106</sup> Eg, Submissions 13, 15, 18, 19. One respondent submitted, however, that this type of exception should be 'mindful' of other included exceptions: Submission 18.

<sup>107</sup> Submission 19.

<sup>108</sup> See QLRC Consultation Paper No 77 (2018) [3.146] and NSWLRC Report No 108 (2005) [5.62]–[5.69], Rec 7. The NSWLRC also recommended that, for other uses of covert surveillance, a private investigator should be required to obtain authorisation.

Queensland insurers and insurance adjusters are not private investigators and do not require a licence, submitted that it:

supports a licensing system being introduced for investigation agents which would ensure that when it is deemed necessary, surveillance can be used to investigate claims in a manner that is appropriate and proportionate.

The Consultation Paper refers to the licensing regime that has been introduced in South Australia. The licensing of investigation agents recognises that surveillance can be used for legitimate purposes, and provides a regulatory framework that balances the need to protect individual privacy with the need for pragmatic rules and certainty around permissible conduct.

5.90 A few respondents submitted more generally that an exception for a person acting in the course of their occupation should include law enforcement agencies other than the police, or permit surveillance conducted ‘by a licensed or authorised individual or agency as part of their duties or for lawful purposes’.<sup>109</sup>

### ***Media organisations and journalists***

5.91 A number of respondents submitted that the use of a surveillance device by a media organisation or journalist acting in the course of their occupation should be permitted, or should not be an offence.<sup>110</sup>

5.92 Future Wise submitted that investigative journalism is a ‘justifiable exception’ to the general principle that surveillance should not be undertaken covertly, but that both the surveillance and any subsequent disclosure should satisfy a public interest test.

5.93 Some respondents, including the QCCL and the QLS, indicated support for an exception for ‘responsible journalism’, as suggested by the ALRC.<sup>111</sup>

5.94 The QCCL stated that ‘the public interest in a free media’ requires protection. This respondent submitted that the media must be capable of investigating issues and informing the public, which requires them to be able to gather evidence, including by covertly recording conversations. On this basis, there should be a ‘specific exception for responsible journalism’.<sup>112</sup>

5.95 The QLS submitted that the use of a surveillance device ‘in the course of responsible journalism intended to serve the public interest’ should be lawful. It stated that:

<sup>109</sup> Eg, Submissions 15, 18 respectively. One respondent also submitted that, for surveillance in public places, a relevant consideration should be whether that surveillance is part of an organisation’s duties. Additionally, for surveillance that is overt or covert, a relevant consideration should be whether the surveillance is conducted by a licensed or authorised agency or individual for ‘lawful purposes’: Submission 18.

<sup>110</sup> Eg, Submissions 13, 15, 18. One respondent submitted, however, that this type of exception should be ‘mindful’ of other included exceptions: Submission 18.

<sup>111</sup> Eg, Submissions 38, 40, 43. As to the ALRC’s proposal, see [5.296]–[5.297] below.

<sup>112</sup> The QCCL described this specific exception as ‘following the lead’ of the ALRC. This respondent also suggested that there should be ‘the safeguard of an enforceable remedy for invasion of privacy’.



The tenets of journalistic independence, subject to reasonable practice and integrity, must be allowed to continue in practice. The Society agrees with the ALRC position that this defence should be constrained and should not allow an unchecked freedom to carry out surveillance in circumstances which do not adhere to the principles of journalistic integrity, or where the public interest is not appropriately served (or circumstances pertaining to smaller matters, including gossip, where there in fact is no reasonable degree of public interest at all).

5.96 An academic suggested adapting the ALRC's proposed defence of responsible journalism into an exception a more general public interest exception that accommodates, but is not limited to, the use of a surveillance device for responsible journalism.<sup>113</sup>

### ***Location and retrieval of a surveillance device***

5.97 Several respondents submitted that the use of a surveillance device in order to locate or retrieve that device should be permitted, or should not be an offence,<sup>114</sup> but another respondent was opposed.<sup>115</sup> The QCCL indicated that this exception would need to be 'drafted in a manner that prevents mission or scope creep'.

5.98 The AAUS stated that surveillance devices legislation should prohibit the use of a surveillance device to determine the geographical location of an object without consent, 'except for the sole purpose of retrieval of that object to its owner'.<sup>116</sup>

### ***Use of a surveillance device in prescribed circumstances***

5.99 A number of respondents submitted that the use of a surveillance device should be permitted, or should not be an offence, where it occurs in some 'prescribed circumstances'.<sup>117</sup> Another respondent was opposed to this approach.<sup>118</sup>

5.100 In this context, some respondents expressed support for the use of a tracking device to:

- track objects that have been stolen, or as an anti-theft measure;<sup>119</sup>

<sup>113</sup> Submission 19, and see also [5.68]–[5.69] above. This respondent also made submissions that limiting this defence to people who are an employee or member of an organisation that has publicly committed to observing standards about the use of surveillance by the media, as suggested by the ALRC, would limit the application of the exception to 'mainstream media'. It would exclude journalists who are not members of an organisation or who engage in forms of journalism, such as blogging. It was suggested that an exception that did not include this limitation 'may be more inclusive and better reflect the realities of modern journalism'.

<sup>114</sup> Eg, Submissions 13, 15, 18, 40.

<sup>115</sup> Submission 22.

<sup>116</sup> AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

<sup>117</sup> Eg, Submissions 13, 15, 19, 40.

<sup>118</sup> Submission 22.

<sup>119</sup> Eg, Submissions 19, 40. One respondent submitted that if the use of a device in circumstances where it has been stolen is not in a person's lawful interests, then there should be a 'narrowly drawn exception for such circumstances': Submission 40. See also AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

- monitor traffic;<sup>120</sup>
- conduct search and rescue operations;<sup>121</sup> or
- monitor the location of a ‘vulnerable person’.<sup>122</sup>

5.101 Some respondents gave particular consideration to the use of tracking and other surveillance devices to monitor patients or vulnerable people. They noted that the use of a tracking device might mitigate risks, but also cautioned that it does not provide an adequate substitute for nursing care or address underlying issues, and has not been proven to increase safety. It was suggested that use in this context should be with a person’s prior consent (for example, through an advanced health directive) or the consent of a substitute decision-maker, or that it should be specifically addressed in separate legislation, such as the *Guardianship and Administration Act 2000* or the *Mental Health Act 2016*. Respondents emphasised the importance of focusing on a person’s safety and wellbeing, and the need to ‘respect the independence of patients’.<sup>123</sup>

5.102 One respondent submitted that there should be a broad prescribed circumstance that protects research conducted using surveillance technologies, subject to approval by an institutional research ethics committee. This would utilise an existing approach that ‘facilitates research and balances privacy against competing interests’, and would offer researchers some protection against liability for inadvertent breaches of privacy.<sup>124</sup>

5.103 Some government departments submitted that legislation about surveillance devices should not impact upon their use of surveillance or their scientific tracking and research, including suggestions that particular uses of surveillance devices by departments should be included as a prescribed circumstance.<sup>125</sup>

### **Other circumstances**

5.104 A number of respondents also suggested additional circumstances for which there could be an exception permitting the use of a surveillance device.

5.105 Some respondents, particularly government departments, submitted that it is necessary to consider the impact of regulation on their use of surveillance to fulfil their obligations, enforce or administer the law, or engage in legitimate and justified

<sup>120</sup> Eg, Submissions 19, 40. In particular, an academic noted that traffic monitoring may be important if automated vehicles are used in Queensland: Submission 19. The QCCL supported traffic monitoring if it was to search for vehicles on a particular list (for example, those that are stolen or unregistered), but opposed a system that is ‘linked to GPS and results in data being added to a database’: Submission 40.

<sup>121</sup> Eg, Submission 40.

<sup>122</sup> Eg, Submissions 19, 32.

<sup>123</sup> Eg, Submissions 21, 33, 40. See also VLRC Report No 18 (2010) [6.48]–[6.53], Rec 17.

<sup>124</sup> Submission 29. See also D Butler and P Meeks, ‘Camera Trapping and Invasions of Privacy: An Australian Legal Perspective’ (2013) 20(3) *Torts Law Journal* 234.

<sup>125</sup> Eg, Submissions 15, 16.

activities that are within their functions. It was submitted that the use of a surveillance devices in such contexts should not be impeded.<sup>126</sup>

5.106 Generally, respondents submitted that the use of a surveillance device should not be prohibited if it is ‘in connection with’, ‘permitted by’, ‘authorised by’ or ‘required by’ a law.<sup>127</sup> For example, the *Fisheries Act 1994* includes provisions that permit or require the use of body-worn cameras and tracking devices.<sup>128</sup> DTMR submitted that this approach is beneficial because ‘it doesn’t require all possible exceptions to be identified in advance’, but it does require the responsible agency to make a robust business case’ that takes into account privacy and other relevant considerations, in the particular circumstances.<sup>129</sup>

5.107 Several respondents submitted that there should be an exception permitting the use of a surveillance device where it is relevant to law enforcement or is in accordance with a person’s occupation or duty, including an occupation or duty that relates to law enforcement.<sup>130</sup> The AAUS suggested that a prohibition should not apply where the installation or use of a surveillance device is ‘by a person acting in their capacity as a police or public officer, provided such conduct was neither disproportionate to the activity nor committed in the course of a trespass’.<sup>131</sup>

5.108 Several government agencies submitted that they should be permitted to use a surveillance device for ‘regulatory’ or ‘enforcement’ purposes, or more broadly for ‘government purposes’. It was also submitted that the use of a device should be permitted in connection with the administration of government, for matters such as site management, protection of tenants, assets or resources, and health or safety.<sup>132</sup>

5.109 One respondent submitted that participant monitoring should not be prohibited for ‘law enforcement purposes’, and another submitted that an exception should permit participant monitoring where it relates to matters of security, emergency or enforcement.<sup>133</sup>

<sup>126</sup> Eg, Submissions 15, 16, 26, 31, 36. One respondent also expressed concerns about the collection, storage and analysis of data: Submission 31.

<sup>127</sup> Eg, Submissions 15, 36, 39.

<sup>128</sup> Submission 15.

<sup>129</sup> Specifically, this respondent suggested an exception ‘where otherwise authorised by law’.

<sup>130</sup> Eg, Submissions 15, 16, 18, 35, 39. One respondent referred specifically to surveillance conducted ‘by a licensed or authorised individual or agency as part of their duties or for ‘lawful purposes’: Submission 18. Another respondent suggested an exception for surveillance that is ‘conducted in the course of official business as an authorised officer under legislative instruments’: Submission 10.

<sup>131</sup> AAUS and Liberty Victoria Paper (2015) [4.3], Rec 3, adopted in Submission 39 from the AAUS.

<sup>132</sup> Eg, Submissions 16, 35. It was also submitted that it might be appropriate to include an exception permitting the gathering of evidence for regulatory and enforcement purposes. See also, eg, Submission 10.

<sup>133</sup> Eg, Submissions 15, 35 respectively. See also [5.42] and n 56, and [5.51]–[5.52] above.

5.110 Some respondents submitted that there could be exceptions permitting the use of a surveillance device for other particular purposes, such as:<sup>134</sup>

- parents using a tracking device, with good intentions, to know where their children are and whether they are safe;<sup>135</sup>
- the collection of scientific data;<sup>136</sup>
- monitoring traffic and enforcing compliance with road rules;<sup>137</sup>
- the use of body-worn cameras (for example, when enforcing traffic laws);<sup>138</sup>
- where the use of a device has a direct relationship to safety or assistance in service delivery, for example, monitoring the security of work sites and buildings or public transport services;<sup>139</sup>
- the protection of the environment;<sup>140</sup> and
- recording activities that are in public places and that are not ‘private acts’, for example, recording activities on waterways, recording boat ramps to monitor and collect data about usage, and covert surveillance of public locations where criminal activity is suspected to be taking place.<sup>141</sup>

## THE COMMISSION’S VIEW

### The approach of the draft Bill

5.111 In the Commission’s view, the regulation of the use of surveillance devices requires a criminal law response to protect the privacy of individuals from unjustified interference.<sup>142</sup>

5.112 Accordingly, the draft Bill prohibits the use of surveillance devices in particular circumstances.

---

<sup>134</sup> DTMR also noted some other current uses of surveillance devices, including the use of roadside tolling equipment to identify and collect tolls from road users, and the provision of vessel tracking services to the maritime industry. Other possible uses include the use of camera technology in-vehicle that captures images of individuals in alcohol ignition interlock programs or to detect and address causes of driver distraction, such as the use of mobile phones. Additionally, vehicle or movement tracking and monitoring can be used to detect heavy vehicles that are not permitted to travel on some roads, or vehicles that are non-compliant.

<sup>135</sup> Submission 27. This respondent (the Women’s Legal Service Qld) observed that this would need to be distinguished from a person who has committed violence against another person, and uses a tracking device to locate that person and/or a child who is fleeing from that violence or hiding out of fear.

<sup>136</sup> Submission 15.

<sup>137</sup> Submission 36.

<sup>138</sup> Ibid. Also, eg, Submissions 15, 31.

<sup>139</sup> Submission 36.

<sup>140</sup> Submissions 15, 36.

<sup>141</sup> Submission 15.

<sup>142</sup> See [3.23]–[3.24] above.

5.113 Specifically, the draft Bill contains four separate use prohibitions, one for each category of surveillance device, which provide that a person must not use, install or maintain:

- a *listening device* to listen to, monitor or record a private conversation, without the consent of each party to the conversation;
- an *optical surveillance device* to observe, monitor or record visually a private activity, without the consent of each party to the activity;
- a *tracking device* to find, monitor or record the geographical location of:
  - an individual, without the consent of the individual; or
  - a vehicle or other thing, without the consent of each person who owns, or is in lawful control of, the vehicle or other thing.
- a *data surveillance device* to access, monitor or record information that is input into, output from or stored in a computer, without the consent of each person who owns, or is in lawful control of, the computer.

5.114 These use prohibitions are subject to exceptions where the use of the surveillance device is for a particular purpose that, in the circumstances, justifies the interference with privacy.<sup>143</sup>

5.115 This approach protects privacy, while taking into account countervailing rights and interests, and is compatible with the *Human Rights Act 2019*.<sup>144</sup> It continues and extends the approach taken in the *Invasion of Privacy Act 1971* and achieves reasonable consistency with the approach taken in the surveillance devices legislation in other jurisdictions.

5.116 The specific aspects of the Commission's approach, including the elements of the use prohibitions and their exceptions, are discussed below.

## ELEMENTS OF THE USE PROHIBITIONS

### Intention

#### **Sections 23 and 24 of the Criminal Code**

5.117 In Queensland, the Criminal Code contains general provisions regarding criminal responsibility, which apply to 'all persons charged with any criminal offence against the statute law of Queensland'.<sup>145</sup> In particular, section 23(1)(b) provides that a person is not criminally responsible for:

an event that—

<sup>143</sup> See further [3.26] above.

<sup>144</sup> *Human Rights Act 2019* (Qld) ss 13, 25.

<sup>145</sup> Criminal Code (Qld) s 36(1). These provisions do not apply to regulatory offences, except in some limited circumstances: s 36(2).

- (i) the person does not intend or foresee as a possible consequence; and
- (ii) an ordinary person would not reasonably foresee as a possible consequence.

5.118 The *Invasion of Privacy Act 1971* provides that a person is guilty of an offence 'if the person uses a listening device' in contravention of the Act.<sup>146</sup> Section 23(1)(b) of the Criminal Code may apply to excuse the person from committing an offence, depending on the particular circumstances.

5.119 This excuse could apply, for example, where a person used a listening device to record a conversation with the consent of the other participants, but the device also recorded another private conversation between other people at the same venue. If the person did not intend or foresee that the listening device would record the second conversation, and provided that the recording of the second conversation would not have been reasonably foreseen by an ordinary person, the person would be excused from criminal responsibility.

5.120 Section 24(1) of the Criminal Code provides that, where a person does (or does not do) an act 'under an honest and reasonable, but mistaken, belief in the existence of any state of things', the person is criminally responsible only to the extent that they would have been if their belief in the state of things was true.<sup>147</sup>

5.121 In the example in [5.119] above, if the person who made the recording honestly and reasonably, but mistakenly, believed that the listening device would not have the capability to record other conversations being held in the same location, the person would be excused from criminal responsibility.

### ***Intention in surveillance devices legislation in other jurisdictions***

5.122 In most jurisdictions, the use prohibitions include an express element of 'intention' or 'knowledge'.

5.123 In the Australian Capital Territory, it is an offence for a person to use a listening device 'with the intention of' acting in a way that is prohibited.<sup>148</sup>

5.124 The surveillance devices legislation in New South Wales, the Northern Territory, South Australia and Victoria includes an element of 'knowledge'.<sup>149</sup> This is

---

<sup>146</sup> *Invasion of Privacy Act 1971* (Qld) s 43(1).

<sup>147</sup> Criminal Code (Qld) s 24(1).

<sup>148</sup> *Listening Devices Act 1992* (ACT) s 4(1). A person has intention if the person means to engage in conduct, means to bring about a result or is aware that it will happen in the ordinary course of events, or believes that a circumstance exists or will exist: *Listening Devices Act 1992* (ACT) s 3A; *Criminal Code 2002* (ACT) s 18.

<sup>149</sup> The term 'knowingly' is defined by the Criminal Code in some jurisdictions. In Queensland, the Criminal Code (Qld) states that '**knowingly**, used in connection with any term denoting uttering or using, implies knowledge of the character of the thing uttered or used': s 1 (definition of 'knowingly').

In the Commonwealth, the Australian Capital Territory and the Northern Territory, a person has knowledge of a result or circumstance if the person is aware that it exists or will exist in the ordinary course of events: *Criminal Code Act 1995* (Cth) s 5.3; *Criminal Code 2002* (ACT) s 19; *Criminal Code Act 1983* (NT) s 43AJ.

expressed in various ways, for example, as knowingly using a device, or as using a device knowing that it is used without consent.<sup>150</sup>

5.125 In the Australian Capital Territory, New South Wales, South Australia, and Tasmania, the use prohibitions do not apply to the unintentional hearing of a conversation by means of a listening device (or, in Western Australia, to the unintentional recording or observation of a private activity).<sup>151</sup> In Queensland, the offence of using a listening device under the *Invasion of Privacy Act 1971* does not include an express element of intention or knowledge, but does not apply to ‘the unintentional hearing of a private conversation by means of a telephone’.<sup>152</sup>

### **No element of intention or exception relating to unintentional use**

5.126 The Commission has considered whether an element of intention or knowledge should be included in the use prohibitions.

5.127 The inclusion of an element of intention or knowledge might be considered useful, given that the concept of ‘surveillance’ is generally understood to involve monitoring for a particular purpose.<sup>153</sup>

5.128 On the other hand, the inclusion of an element of intention or knowledge would narrow the scope of the use prohibitions. For example, a recreational drone flyer who flies a drone around or over a person’s house and captures images of private activities may not intend to observe or record those activities, even though an ordinary person would reasonably foresee such capture as a possible consequence. A specific element of knowledge or intention might erode the reasonable regulation of some uses of surveillance devices.

5.129 In the Commission’s view, the availability of section 23(1)(b) of the Criminal Code as an excuse of general application makes it unnecessary to include an express element of intention or knowledge in each of the offences created by the use prohibitions in the draft Bill.<sup>154</sup> Applying section 23(1)(b), a person would be excused from criminal responsibility for a contravention of a use prohibition under the draft Bill if they did not intend or foresee an event as a possible consequence, and an ordinary person would not reasonably foresee the event as a possible consequence.

<sup>150</sup> *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); *Surveillance Devices Act 2016* (SA) ss 4(1), 5(1)–(3), 7(1), 8(1); *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(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).

<sup>151</sup> *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).

<sup>152</sup> *Invasion of Privacy Act 1971* (Qld) s 43(2)(b).

<sup>153</sup> See [2.1] above. The ACT Review, the NSWLRC and the VLRC conceptualised ‘surveillance’ as involving deliberate monitoring: QLRC Consultation Paper No 77 (2018) [2.23].

<sup>154</sup> MJ Shanahan et al, Lexis Nexis Australia, *Carter’s Criminal Law of Queensland* (at April 2018) [2.3.1]. An intention to cause a specific result may sometimes be included in an offence, for example, the intent to cause death: s 302.

5.130 The Commission notes that the Western Australian Criminal Code includes provisions similar to sections 23 and 24.<sup>155</sup> The surveillance devices legislation in that jurisdiction (which has been expanded beyond listening devices) does not include an element of intention or knowledge, but does include exceptions relevant to the use of a listening device or an optical surveillance device that results in the unintentional hearing of a private conversation, or the unintentional recording or observation of a private activity.

5.131 In the Commission's view, the scope of the excuses provided by sections 23 and 24 of the Criminal Code is sufficient protection for the unintentional prohibited use of a surveillance device.

5.132 Sections 23 and 24 of the Criminal Code will apply to the offences created by the use prohibitions for each category of surveillance device in a consistent way. In contrast, exceptions for unintentional use in other jurisdictions apply only to a listening device or an optical surveillance device, and to only some of the prohibited uses for those devices.

### **Use, install or maintain surveillance devices**

5.133 The use prohibitions in the draft Bill apply to the use, installation or maintenance of a surveillance device.

5.134 The *Invasion of Privacy Act 1971* does not define the word 'use', but in some other jurisdictions 'use' of a surveillance device 'includes use of the device to record a conversation or other activity'.<sup>156</sup>

5.135 The ordinary meaning of 'use' includes putting something into action or service, or carrying out a purpose or action by means of a particular thing.<sup>157</sup> Common examples of the 'use' of a device might be a person using their mobile phone to make an audio recording of a conversation, or using a video camera to record an event.

5.136 As a general approach, words or phrases in the draft Bill should be given their ordinary, plain English meaning and should not be defined unless it is necessary to do so.<sup>158</sup> Consistently with the current legislation and with this general approach, it is not necessary to define the word 'use'.

---

<sup>155</sup> *Criminal Code Act Compilation Act 1913* (WA) ss 23, 24.

<sup>156</sup> 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).

<sup>157</sup> Merriam-Webster Dictionary (online at 24 February 2020) 'use'; Oxford Dictionary (online at 24 February 2020) 'use'; Macquarie Dictionary (online at 24 February 2020) 'use'. See also QLRC Consultation Paper No 77 (2018) [3.53]–[3.54].

<sup>158</sup> See generally Office of the Queensland Parliamentary Counsel, *Principles of good legislation: OQPC guide to FLPs*, 'Clear meaning' (14 February 2014) [6] ff.



5.137 The term ‘maintain’ is defined in surveillance devices legislation in other jurisdictions to include adjusting, relocating or repositioning, repairing and servicing a surveillance device, or replacing a faulty device.<sup>159</sup> 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.

5.138 The ordinary meaning of ‘maintain’ is to enable something to continue in its existing state, including by keeping something in good condition by conducting regular checks and repairs.<sup>160</sup>

5.139 The draft Bill provides that ‘maintain’, in relation to a surveillance device, includes adjusting, relocating, repairing and servicing the device, or replacing a device that is faulty. This makes it clear that the action of replacing a faulty surveillance device does not amount to the installation of a surveillance device, and is consistent with the definition of ‘maintain’ in surveillance devices legislation in other jurisdictions.

5.140 Another relevant matter is doing something to or in relation to a device, for example, the installation of a program on an individual’s smartphone that tracks the individual’s location without their consent.

5.141 In some jurisdictions, the legislation defines the word ‘install’ to include ‘attach’.<sup>161</sup> In Queensland, the PPRA 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 connecting the device to another device using a wireless connection.<sup>162</sup>

5.142 This provision was inserted into the PPRA to:<sup>163</sup>

clarify that a reference ... to installation of a surveillance device is taken to include a reference to doing anything to an existing device, including the covert manipulation of the device either physically or remotely and including the remote installation of software, to enable the device to be used as a surveillance device. This clause, in conjunction with clauses [about existing devices], [clarifies] that a

---

In some jurisdictions surveillance devices legislation also refers to a device being ‘caused’ or ‘permitted’ to be used. In New South Wales and South Australia, a person must not ‘use or cause to be used’ a listening device, and, in Tasmania, a person must also not ‘permit’ the use of a listening device. In Western Australia, a person must not cause any of the included devices to be used, installed, maintained or, for tracking devices, attached: *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).

In circumstances where another person causes or permits the unlawful use, installation or maintenance of a surveillance device, the provisions of the Criminal Code relevant to charging and convicting principal offenders will apply: Criminal Code (Qld) s 7, and see [5.279] below.

159 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). In Western Australia, the definition does not include replacement of a device.

160 Merriam-Webster Dictionary (online at 24 February 2020) ‘maintain’; Oxford Dictionary (online at 24 February 2020) ‘maintain’; Macquarie Dictionary (online at 24 February 2020) ‘maintain’.

161 See the definition of ‘install’ in *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; and *Surveillance Devices Act 1999* (Vic) s 3(1).

162 *Police Powers and Responsibilities Act 2000* (Qld) s 324A.

163 Explanatory Memorandum, Counter-Terrorism and Other Legislation Amendment Bill 2017 (Qld) 26.

surveillance device warrant, emergency authorisation or tracking device authorisation can authorise an existing device within the target premises, in possession of a person or in a vehicle or object, as a surveillance device or type of surveillance device.

5.143 The draft Bill includes a provision explaining the word ‘install’, in similar terms to the PPRA provision.

5.144 It is not necessary to separately refer to the attachment of a surveillance device, or to define the word ‘install’ to include attachment. The word ‘install’ is broad enough to capture attaching a device to another thing, for example, attaching a device to clothing to enable the device to be worn.

### Prohibited uses

5.145 The use prohibitions in the draft Bill are generally consistent with those in surveillance devices legislation in other jurisdictions, namely: to listen to, observe, monitor or record conversations and activities; to access, monitor or record information that is input into, output from or stored in a computer; and to track the geographical location of an individual, vehicle or other thing.<sup>164</sup>

5.146 In other jurisdictions, terms such as ‘record’, ‘observe’, ‘monitor’, ‘access’ or ‘track’ are not defined by the legislation. These prohibited uses are self-explanatory and do not need to be defined in the draft Bill.

5.147 For each of the use prohibitions, an element of the offence is that the installation, use or maintenance of the surveillance device occurs without consent. The particular requirements for consent vary, depending on the type of surveillance device. Those requirements are discussed separately below.<sup>165</sup>

### Listening devices

5.148 In relation to a listening device, the draft Bill prohibits the use, installation or maintenance of a listening device to listen to, monitor or record a private conversation.<sup>166</sup>

5.149 Some jurisdictions (including Queensland) prohibit the use of a listening device to ‘overhear’ a private conversation.<sup>167</sup> Other jurisdictions prohibit the use of a listening device to ‘listen to’ a private conversation and define the term ‘listening to’ as including ‘hear’.<sup>168</sup>

---

<sup>164</sup> See further, [2.27] ff and [5.5] above.

<sup>165</sup> See [5.204] ff below.

<sup>166</sup> As to the term ‘private conversation’, see [5.162] ff below.

<sup>167</sup> *Surveillance Devices Act 2007* (NSW) s 7(1); *Invasion of Privacy Act 1971* (Qld) s 43(1); *Surveillance Devices Act 2016* (SA) s 4(1); *Surveillance Devices Act 1999* (Vic) s 6(1). See also *Police Powers and Responsibilities Act 2000* (Qld) sch 6 (definition of ‘listening device’).

<sup>168</sup> See the definition of ‘listen to’ in *Listening Devices Act 1992* (ACT) s 2, Dictionary; *Surveillance Devices Act* (NT) s 4; *Listening Devices Act 1991* (Tas) s 3(1); and *Surveillance Devices Act 1998* (WA) s 3(1).

5.150 The Commission considers that a prohibition on the use of a listening device to 'listen to' a private conversation is reasonable. The ordinary meaning of 'listen to' is wide enough and does not require further definition.

5.151 The use of a listening device to 'overhear' a private conversation should not be included as a prohibited use. A person may 'overhear' a private conversation inadvertently or unintentionally, and it is not intended that the unintentional use of surveillance devices be captured as an offence.

### ***Optical surveillance devices***

5.152 The draft Bill prohibits the use, installation or maintenance of an optical surveillance device to observe, monitor or record visually a private activity.<sup>169</sup> This is consistent with the approach taken in relation to the use of a listening device.

### ***Tracking devices***

5.153 Similarly to surveillance devices legislation in other jurisdictions, the draft Bill prohibits the use, installation or maintenance of a tracking device to find, monitor or record the geographical location of an individual, vehicle or other thing.

### ***Data surveillance devices***

5.154 The draft Bill prohibits the use, installation or maintenance of a data surveillance device to access, monitor or record information that is input into, output from or stored in a computer.

5.155 The scope of the use prohibitions for a data surveillance device varies between jurisdictions. In New South Wales, it is an offence for a person to monitor or record the input of information into, or the output of information from, a computer.<sup>170</sup> The legislation in South Australia also prohibits accessing or tracking information, and extends to information stored in a computer.<sup>171</sup>

5.156 The prohibition in the draft Bill protects against the use of a data surveillance device to access information that is stored in a computer. It is likely that, when a data surveillance device is used, information that should reasonably be protected will already have been stored on that computer; if the prohibition were limited to information input into or output from a computer, 'stored' information would not be protected. It is sufficient to prohibit accessing, monitoring and recording information, and is unnecessary to also include the tracking of information as a prohibited use.

5.157 Depending on the circumstances, offences under the *Telecommunications (Interception and Access) Act 1979* (Cth) and offences in relation to accessing or

<sup>169</sup> As to the term 'private activity', see [5.173] ff below.

<sup>170</sup> *Surveillance Devices Act 2007* (NSW) s 10(1). Legislation in the Northern Territory and Victoria includes the same prohibitions, but they apply to law enforcement officers only: *Surveillance Devices Act* (NT) s 14(1); *Surveillance Devices Act 1999* (Vic) s 9(1).

<sup>171</sup> *Surveillance Devices Act 2016* (SA) s 8(1).

'hacking' information stored in a computer may also apply.<sup>172</sup> However, in the Commission's view, it is appropriate that the law provides for broader protections against the use of a data surveillance device.<sup>173</sup>

### Private conversations and activities

5.158 The concepts of 'private conversation' and 'private activity' are fundamental to the regulation of the use of a listening device and an optical surveillance device, respectively.

5.159 Generally, a 'private conversation' or a 'private activity' is one that occurs between two or more people in circumstances that may reasonably be taken to indicate that the people who are speaking or being spoken to, or participating in an activity, 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.<sup>174</sup> 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.<sup>175</sup>

5.160 In Queensland, the *Invasion of Privacy Act 1971* defines the term 'private conversation' to mean:<sup>176</sup>

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.

5.161 In other jurisdictions, the courts have held that a conversation is 'private' if it is 'intended to be confined to the parties', and can be private even where the parties

<sup>172</sup> See [D.4]–[D.14], [D.44] below. In relation to the offence of computer hacking or misuse under s 408E of the Criminal Code (Qld), it is a defence to a charge under s 408E to prove that a person's use of a restricted computer without the consent of the computer's controller was authorised, justified or excused by law: s 408E(4).

<sup>173</sup> See further [4.68] ff above.

<sup>174</sup> See the definitions of 'private conversation' and 'private activity', as relevant, in *Listening Devices Act 1992* (ACT) s 2, Dictionary; *Surveillance Devices Act 2007* (NSW) s 4(1); *Surveillance Devices Act* (NT) s 4; *Invasion of Privacy Act 1971* (Qld) 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); and *Surveillance Devices Act 1998* (WA) s 3(1). The legislation in Queensland, the Australian Capital Territory, New South Wales and Tasmania defines 'private conversation' only. See also [2.21], [2.32]–[2.33] above.

In Queensland, the term 'reasonably' is used only in relation to the latter of these circumstances: *Invasion of Privacy Act 1971* (Qld) s 4 (definition of 'private conversation').

<sup>175</sup> *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'); *Invasion of Privacy Act 1971* (Qld) s 42(2); *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'). See also [2.23], [2.34]–[2.35] above.

<sup>176</sup> *Invasion of Privacy Act 1971* (Qld) s 4 (definition of 'private conversation').

are permitted to tell other people about it afterwards. In the context of surveillance devices legislation, “private” is used not in the sense of “secret” or “confidential”, but in the sense of “not public”.<sup>177</sup>

### **Private conversations**

5.162 The draft Bill defines the term ‘private conversation’ as follows:

Words spoken by an individual are a **private conversation** if the words are spoken in circumstances that may reasonably be taken to indicate that—

- (a) for words not spoken to anyone else—the individual does not want anyone else to listen to the words; or
- (b) for words spoken to another individual, or other individuals—the individual, or at least 1 of the individuals to whom the words are spoken, does not want the words to be listened to by anyone other than—
  - (i) the individual speaking the words; and
  - (ii) the individuals to whom the words are spoken; and
  - (iii) any other individual who has the consent of all of the individuals mentioned in paragraphs (a) and (b).

However, a **private conversation** does not include words spoken by an individual in circumstances in which the individual, and all of the individuals to whom the words are spoken, ought reasonably to expect that someone else may listen to, monitor or record the words.

5.163 This definition has two limbs. The first limb extends the current definition in Queensland. It relates to words spoken by one person who does not want the words to be listened to by any other person. Circumstances might arise, for example, where a person is dictating private information into a computer.

5.164 The Commission considers that this additional limb is necessary to ensure that a communication involving one person only is adequately protected in appropriate circumstances.

5.165 The second limb deals with private communications that are between two or more people. This limb draws on the definitions of ‘private conversation’ presently

<sup>177</sup> *Thomas v Nash* (2010) 107 SASR 309, [36]–[38], cited with approval in *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [23]–[24] and *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd* (2018) 132 SASR 63, 85 [80].

Consideration has also been given to the concept of a ‘private conversation’ in the context of a business or committee meeting. Generally, formal and structured meetings that have a commercial character or purpose can be ‘private’ but may not have the characteristics of a ‘conversation’. See *Alliance Craton Explorer Pty Ltd v Quasar Resources Ltd* [2010] SASC 266, cited in *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd* (2018) 132 SASR 63, 85–88 [82]–[90] and *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [20]–[21].

included in the *Invasion of Privacy Act 1971*,<sup>178</sup> the PPRA<sup>179</sup> and the surveillance devices legislation in other jurisdictions.<sup>180</sup>

5.166 The proposed definition of ‘private conversation’ differs from the current definitions in the *Invasion of Privacy Act 1971* and the PPRA by referring in both limbs to ‘circumstances that *may reasonably be taken to indicate*’. The words ‘may reasonably be taken to’ add an objective test that can be applied in a practical way when considering the limits of the use prohibitions. The addition of those words is consistent with surveillance devices legislation in other jurisdictions.

5.167 The second limb of the proposed definition of ‘private conversation’ refers to ‘words spoken by one person to another person, or other persons’, and not to ‘a conversation’. This extends the ordinary meaning of ‘conversation’ to an instance where only one person speaks aloud, such as where an instruction is given to another person. It also reflects that a conversation may be between two or more persons.

5.168 The second limb also recognises that the persons engaged in a conversation can include the persons who are speaking or are directly spoken to, as well as other people who are listening to the conversation.<sup>181</sup> Sometimes, a person’s role in a conversation will become apparent only as the conversation progresses. For example, a person might be invited to listen to a conversation but then be called upon to speak, or be invited to be a part of a conversation in which they were not ultimately required to speak.

5.169 The Commission’s view is that the persons engaged in a private conversation should be treated equally, because they all have an involvement and an interest in the conversation. The interests of each person might differ, but each interest should be recognised.

5.170 Both limbs are subject to the limitation that the term ‘private conversation’ does not include words spoken in circumstances where it ought reasonably to be expected that the words may be listened to, monitored or recorded by someone else.

5.171 In relation to the second limb, a conversation will be a private conversation if the circumstances may reasonably be taken to indicate that any one of the persons speaking or being spoken to wants the conversation to be listened to only by themselves, or by themselves and others who are listening with their consent. However, it will not be a private conversation if, in the circumstances, all of the persons speaking or being spoken to (including a person who wanted the

<sup>178</sup> *Invasion of Privacy Act 1971* (Qld) s 4.

<sup>179</sup> *Police Powers and Responsibilities Act 2000* (Qld) sch 6.

<sup>180</sup> See the definitions of ‘private conversation’ and ‘private activity’ as relevant in *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). In the ACT Review, it was recommended that the definitions of ‘private conversation’ and ‘private activity’ should not include circumstances ‘where the parties can reasonably expect to be overheard or observed by others’: ACT Review [2.5](b), [6.7].

<sup>181</sup> A person might listen to a conversation by being present for it, or by using a listening device. For example, a person might listen to a conversation using a telephone.

conversation to be private) ought reasonably to have expected that the conversation might be listened to, monitored or recorded by someone else.

5.172 The limitation refers to an expectation that words may be ‘listened to, monitored or recorded’ by someone else. This is consistent with the *Invasion of Privacy Act 1971* and the PPRA.<sup>182</sup> Given the increasing use of surveillance devices in the community, it is appropriate that considerations of what is a ‘private conversation’ include the circumstances in which a person ought reasonably to expect that they might be monitored or recorded.

### **Private activities**

5.173 The draft Bill defines the term ‘private activity’ as follows:

An activity is a **private activity** if it is carried out in circumstances that may reasonably be taken to indicate that—

- (a) for an activity carried out by 1 individual—the individual does not want anyone else to observe the activity; or
- (b) for an activity carried out by 2 or more individuals—at least 1 of the individuals does not want the activity to be observed by anyone other than—
  - (i) the individuals carrying out the activity; and
  - (ii) any other individual who has the consent of all of the individuals carrying out the activity.

However, a **private activity** does not include an activity carried out by 1 or more individuals in circumstances in which all of the individuals carrying out the activity ought reasonably to expect that someone else may observe, monitor or visually record the activity.

5.174 The definition of ‘private activity’ is consistent with the definition of ‘private conversation’ in the draft Bill, and with the approach taken in the surveillance devices legislation in other jurisdictions.

5.175 A ‘private activity’ can be engaged in by one person, or by more than one person. In either instance, similarly to a private conversation, an activity can be a private activity if the circumstances may reasonably be taken to indicate that the person, or any of the participants, want the activity to be observed only by themselves, or by themselves and others who are observing with consent. An activity may not be private if the person or all of the participants ought reasonably to have expected that it may be observed, monitored or visually recorded by someone else.

5.176 Like the definition of ‘private conversation’, this definition recognises that the persons who engage in an activity can include those who participate directly in the activity and others who observe the activity.<sup>183</sup> A person’s role in an activity might

<sup>182</sup> Consistency with the *Police Powers and Responsibilities Act 2000* (Qld) is important. The draft Bill includes an exception for use of a surveillance device that is authorised under another Act (see [5.339] ff below), which will encompass use of a surveillance device under the *Police Powers and Responsibilities Act 2000* (Qld).

<sup>183</sup> A person might observe an activity by being physically present for it, or by using an optical surveillance device. For example, a person might observe an activity using Skype.

become apparent only as that activity progresses. All of the persons engaged in a private activity should be treated equally because they all have an involvement and an interest in the activity.

5.177 In South Australia, a private activity does not include an activity that is carried on in a public place, or in premises or a vehicle if it can be readily observed from a public place.<sup>184</sup> In Victoria, a private activity does not include an activity carried on outside a building.<sup>185</sup> The VLRC recommended that the definition of private activity be amended to remove this limitation, observing that this would ensure consistency in the regulation of listening devices and optical surveillance devices.<sup>186</sup>

5.178 These types of restrictions do not apply to the definition of ‘private activity’ in the draft Bill. There are circumstances in which a private activity might reasonably be carried out in a place that could be considered ‘public’ or that is outside (for example, two people might agree to meet in a secluded public area). Some places that are outside a building might be considered ‘private’, such as a backyard swimming pool. Additionally, excluding activities that participants ‘ought reasonably to expect may be observed, monitored or recorded’ adequately provides for any activities that might be seen from a public place.

### ***Other conversations and activities***

5.179 The Commission considered suggestions for a legislative scheme that applies to all conversations and activities, or to a broader range of conversations and activities.<sup>187</sup> However, there is a risk that, if the legislation applied more broadly, or required more detailed consideration of whether each conversation or activity was private, it would be unclear and difficult to enforce.

5.180 The draft Bill regulates the use of a listening device and an optical surveillance device in relation to a ‘private conversation’ and a ‘private activity’. This protects individuals’ right to privacy, whilst taking account of countervailing rights and interests, and other legitimate uses of those devices.

### ***Alternative regulation of optical surveillance devices: ‘property-based approach’***

5.181 In the Northern Territory, Victoria and Western Australia, the use prohibitions for a listening device and an optical surveillance device are in similar

<sup>184</sup> *Surveillance Devices Act 2016* (SA) s 3(1) (definition of ‘private activity’). A ‘public place’ is defined in s 3(1) as including:

- (a) a place to which free access is permitted to the public, with the express or tacit consent of the owner or occupier of that place; and
- (b) a place to which the public are admitted on payment of money, the test of admittance being the payment of money only; and
- (c) a road, street, footway, court, alley or thoroughfare which the public are allowed to use, even though that road, street, footway, court, alley or thoroughfare is on private property.

<sup>185</sup> *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of ‘private activity’). The term ‘building’ includes any structure: s 3(1) (definition of ‘building’).

<sup>186</sup> VLRC Report No 18 (2010) [6.7]–[6.14], Rec 11, and generally [5.11]–[5.15].

<sup>187</sup> See, eg [5.23]–[5.24] above.



terms, with the prohibition for an optical surveillance device taking an ‘activity-based approach’. Generally, it is an offence for a person to use, install or maintain an optical surveillance device to observe, monitor or record visually a private activity, without the consent of each party.<sup>188</sup>

5.182 In New South Wales and South Australia, the use prohibitions for an optical surveillance device take (in whole or in part) a ‘property-based approach’.

5.183 In New South Wales, a person must not knowingly install, use or maintain an optical surveillance device on or within premises, a vehicle or any other object to observe or record visually an activity, if that involves:<sup>189</sup>

- entry onto or into the premises or vehicle without the consent of the owner or occupier of the premises or vehicle; or
- interference with the vehicle or other object without the consent of the person having lawful possession or lawful control of the vehicle or object.

5.184 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’.<sup>190</sup>

5.185 In South Australia, the prohibition incorporates both an activity-based and a property-based approach. A person must not knowingly use, install or maintain an optical surveillance device on or in premises, a vehicle or any other thing, to observe or record visually a private activity:<sup>191</sup>

- without the consent of each party to the activity (whether or not the person has lawful possession or lawful control of the premises, vehicle or thing); and
- if the installation, use or maintenance involves entry onto or into the premises or vehicle, without the consent of the owner or occupier of the premises or vehicle; and

<sup>188</sup> *Surveillance Devices Act* (NT) s 12(1); *Surveillance Devices Act 1999* (Vic) s 7(1); *Surveillance Devices Act 1998* (WA) ss 6(1), (3)(a). In jurisdictions where participant monitoring is permitted, the offence relates only to a private activity to which a person is not a party: see further [5.245] ff below.

Similarly, it is an offence for a person to use, install or maintain a listening device to listen to, monitor or record a private conversation, without the consent of each party: see [5.207] ff below.

<sup>189</sup> *Surveillance Devices Act 2007* (NSW) s 8(1). This prohibition is not restricted to a ‘private activity’. ‘Premises’ is defined to include land, a building, a part of a building and any place, whether built on or not, whether in or outside the jurisdiction; ‘vehicle’ is defined to include an aircraft, a vessel or a part of a vehicle, whether in or outside of the jurisdiction: s 4(1) (definitions of ‘premises’ and ‘vehicle’).

<sup>190</sup> New South Wales, *Parliamentary Debates*, Legislative Assembly (6 November 2007) 3579 (D Campbell, Minister for Police and Minister for the Illawarra). See also New South Wales, *Parliamentary Debates*, Legislative Council (14 November 2007) 4045 (L Rhiannon) and 4049 (J Hatzistergos, Attorney-General and Minister for Justice). This explanation applies to the approach taken for optical surveillance devices, tracking devices and data surveillance devices.

<sup>191</sup> *Surveillance Devices Act 2016* (SA) ss 5(1)–(3). ‘Premises’ is defined to include land, a building, a part of a building and any place, whether built on or not, whether in or outside the jurisdiction; ‘vehicle’ is defined to include any vessel or aircraft: s 3(1) (definitions of ‘premises’ and ‘vehicle’).

- if the installation, use or maintenance involves interference with the premises, vehicle or thing, without the consent of the person having lawful possession or lawful control of the premises, vehicle or thing.

5.186 In the Commission's view, a strict property-based approach could have undesirable outcomes. For example, the owner of a house could use an optical surveillance device to record other occupants or visitors without their knowledge, or a person could use a surveillance device on their own property to record neighbouring premises without entry or interference. Criminal offences that prohibit observation or recording will protect some types of private activities, such as undressing or bathing,<sup>192</sup> but not other activities that might be considered private, for example, receiving medical care at home, engaging in an activity associated with religious observance or working on a confidential project.

5.187 The consent of people who are participating in an activity that is being observed, monitored or recorded is of critical importance.<sup>193</sup> This is not addressed by a property-based approach. Additionally, the need for consent of an owner or occupier, or a person in lawful possession or lawful control, might create difficulties in some circumstances, such as where those persons are not easily identifiable.

5.188 As discussed previously, the use prohibition for an optical surveillance device in the draft Bill is directed to private activities, which are protected regardless of the location in which they occur.<sup>194</sup> Accordingly, the draft Bill does not take an approach that turns, in whole or in part, on the location of the device user or the existence of an entry or interference occurring without consent. Uses of an optical surveillance device that do not capture private activities, such as taking photographs in the open at a tourist attraction or using a dashboard-mounted camera whilst driving on a public road, would not be captured by the prohibition.

5.189 The Commission has considered whether the draft Bill should incorporate both an activity-based and a property-based approach. However, it is not intended to permit or create specific laws about the use of a surveillance device in homes or premises, or to regulate trespass or interference with property. An activity-based approach would best reflect the intended purpose of the draft Bill, namely to protect the privacy interests of people engaged in private activities.

5.190 For these reasons, the use prohibition for an optical surveillance device is based on an activity-based approach. Additionally, so far as it is appropriate, the use prohibitions for a listening device and an optical surveillance device, including any exceptions, are consistent.

## Tracking devices and data surveillance devices

5.191 In the surveillance devices legislation in other jurisdictions, the regulation of the use of a listening device or an optical surveillance device is generally limited in application to a 'private conversation' or a 'private activity'. In comparison, the

<sup>192</sup> See, eg, Criminal Code (Qld) ss 223, 227A, 229A, and [D.32] ff below.

<sup>193</sup> See also [5.204] ff below, as to consent.

<sup>194</sup> See [5.173] ff above.

regulation of the use of a tracking device or a data surveillance device applies whether or not the relevant information or location is ‘private’.

5.192 This approach more closely reflects the reality that listening devices and optical surveillance devices are used in many aspects of everyday life, and in ways that are often widely accepted. For example, it is common for people to make audio or audio-visual recordings of events that they attend, or to take photographs in public settings and at some private events.

5.193 In comparison, there may be greater expectations of privacy associated with tracking devices and data surveillance devices. It has been observed that these devices can provide a wide range of information about a person, and that their use can amount to a significant interference with an individual’s privacy.<sup>195</sup> Additionally, there is not a reasonably clear dividing line between when information obtained using a data surveillance device or a tracking device would or would not be considered private, because what is ‘private’ will depend upon an individual’s circumstances.

5.194 In the Northern Territory and Victoria, the regulation of data surveillance devices applies to law enforcement officers only. Both jurisdictions acknowledged that these devices might be used for legitimate purposes, and the Northern Territory explained that this made it ‘unreasonable to criminalise all use’.<sup>196</sup>

5.195 On balance, the Commission is of the view that tracking devices and data surveillance devices should be regulated broadly, by prohibiting the use of those devices without consent as the starting point, but with appropriate exceptions.

## Parties

5.196 A ‘party’ to a private conversation is defined in surveillance devices legislation:<sup>197</sup>

- 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);

<sup>195</sup> See, eg, ACT Review (2016) [6.8]; VLRC, Report No 18 (2010) [6.29]–[6.30]; NZLC Report No 113 (2010) [3.50]–[3.51]; NSWLRC Interim Report No 98 (2001) [2.15], [2.69], [2.73]. On the other hand, regulation of tracking devices and data surveillance devices could be approached on the basis that those devices should not be subject to any greater restrictions: see, eg, NSWLRC Interim Report No 98 (2001) [2.15], and at [2.69], [2.73]; Joint Working Group Discussion Paper (February 2003) 227, 229.

<sup>196</sup> *Surveillance Devices Act* (NT) s 14; *Surveillance Devices Act 1999* (Vic) s 9; Explanatory Statement, *Surveillance Devices Bill 2007* (NT), cl 14; Northern Territory, *Parliamentary Debates*, Legislative Assembly, 20 June 2007, 4760 (S Stirling, Minister for Justice and Attorney-General); Department of Justice Victoria, *Surveillance Devices Bill*, Discussion Paper (July 1998) 7; Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 547 (Mr Hulls).

Previously, legislation in the Northern Territory prohibited the installation, use or maintenance of a data surveillance device by any person: *Surveillance Devices Act 2000* (NT) s 5 (repealed).

<sup>197</sup> *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’).

- in Queensland, the Australian Capital Territory, New South Wales, Tasmania and Western Australia 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.

5.197 A ‘party’ to a private activity is generally defined as a person who takes part in the activity.<sup>198</sup> 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.<sup>199</sup>

5.198 The draft Bill defines the term ‘party’ as:

Each of the following is a **party** to a private conversation—

- (a) an individual who speaks, or is spoken to, during the conversation;
- (b) an individual who listens to the conversation with the consent of all of the individuals mentioned in paragraph (a).

Each of the following is a **party** to a private activity—

- (a) an individual carrying out the activity;
- (b) an individual who observes the activity with the consent of all of the individuals mentioned in paragraph (a).

5.199 The definitions of ‘private conversation’ and ‘private activity’ in the draft Bill recognise that the people engaged in a conversation or an activity include the people who are speaking or being spoken to in a conversation, or the people who are participating in an activity, and the people who are permitted to listen to or observe the conversation or activity.<sup>200</sup>

5.200 As mentioned earlier, the Commission considers that all of those people should be treated equally, because they all have an involvement and an interest in the conversation or activity.<sup>201</sup> In particular, each person should be able to protect their interests by having a role in consenting to the use of a listening device or an optical surveillance device in connection with the conversation or activity.

5.201 Accordingly, each person who is speaking or being spoken to in a conversation, participating in an activity, or permitted to listen to or observe the conversation or activity, should be a ‘party’ to that conversation or activity under the

<sup>198</sup> *Surveillance Devices Act* (NT) s 4 (definition of ‘party’); *Surveillance Devices Act 1999* (Vic) s 3(1) (definition of ‘party’). See also, in similar terms, *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of ‘party’) which applies in relation to an ‘activity’.

<sup>199</sup> *Surveillance Devices Act 1998* (WA) s 3(1) (definitions of ‘party’ and ‘principal party’). The term ‘principal party’ is not used in New South Wales or South Australia in relation to activities. This might be because the legislation takes, in whole or in part, a property-based approach to regulation of optical surveillance devices, which makes differentiation between principal and other parties unnecessary.

<sup>200</sup> A person might listen to or observe a conversation or an activity by being present for it, or by using a listening device or an optical surveillance device.

<sup>201</sup> See [5.168]–[5.169], [5.176] above.

draft Bill. The use of a listening device or an optical surveillance device is not unlawful if it is with the consent of each party to a private conversation or a private activity.<sup>202</sup>

5.202 A person who monitors or records a private conversation or private activity will not be a party to it, unless they also have another role in the conversation or activity.<sup>203</sup> For example, a person might listen to a private conversation with consent and also use a listening device to record that private conversation. In that instance, the person would be a party because they are listening to the conversation with consent.<sup>204</sup>

5.203 The concept of parties is not applicable to the regulation of a tracking device or a data surveillance device.

## Consent

5.204 Consent is a key concept informing the Commission's view and the development of the draft Bill.<sup>205</sup>

5.205 Each of the use prohibitions in the draft Bill include a lack of consent as an element of the offence, rather than including consent as an exception to the offence. This reduces the scope of uses that are *prima facie* unlawful, and makes it clear that non-consensual use is unlawful unless an exception applies. A person who uses a surveillance device with consent will not commit an offence.<sup>206</sup>

5.206 The use of a surveillance device with consent, which may be express or implied, is generally permitted by surveillance devices legislation in other jurisdictions.<sup>207</sup>

## Listening devices and optical surveillance devices

5.207 In some jurisdictions, consent is an integral part of the definitions of the terms 'private conversation', 'private activity' and 'party'. Generally, a conversation may be private if the parties want it to be heard only by themselves, or by themselves and another person with their consent. A person may be a party to a private

<sup>202</sup> See [5.207] ff below as to consent. This view takes into account the practicalities that there may be circumstances in which a person's role in a conversation or activity may become clear only as the conversation or activity progresses. A person might intend to speak but only listen, or might attend to listen and then be called upon to speak.

<sup>203</sup> Accordingly, a person who monitors or records a private conversation or private activity, without having any other role in that conversation or activity, will not be able or required to give or refuse consent to the use of a listening device or an optical surveillance device.

<sup>204</sup> A person who listens to a private conversation with the requisite consent would be a party to the conversation regardless of whether their use of a listening device to record that conversation was lawful or unlawful. In either instance, the person would be listening to the conversation with consent.

<sup>205</sup> See [3.18]–[3.19] and [4.99] ff above.

<sup>206</sup> Under the draft Bill, 'consent' is defined as express or implied consent: see [4.100] above, Rec 4-11.

<sup>207</sup> *Listening Devices Act 1992* (ACT) s 2 Dictionary (definition of 'consent'), s 4(3)(a); *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). See also *Invasion of Privacy Act 1971* (Qld) ss 42(2)(b), 43(2)(a).

conversation or activity if they are present to listen, observe or record with the consent of the principal parties.<sup>208</sup>

5.208 In most jurisdictions, a person is not prohibited from using a listening device or an optical surveillance device to listen to, observe, monitor or record a private conversation or activity if that is done with the consent of the principal parties. Consent is included as an exception to the use prohibitions for a person who is a party to a conversation or activity,<sup>209</sup> or a lack of consent is included as an element of the relevant offence.<sup>210</sup>

5.209 The draft Bill generally prohibits the use of a listening device or an optical surveillance device without the express or implied consent of each 'party'.<sup>211</sup>

5.210 In effect, this requires the consent of each person who is engaged in a private conversation or a private activity; namely each person who is speaking or being spoken to in a conversation or participating in an activity, and each person who is listening to or observing a conversation or activity with consent.

5.211 This approach treats each of those persons in the same way, recognising that they all have an interest in the conversation or activity and should all be able to protect their interest by having a role in consenting to the use of a listening device or an optical surveillance device.<sup>212</sup> This might be of particular relevance for the use of an optical surveillance device, where every person could be seen as being present in a visual recording.

### Tracking devices

5.212 In other jurisdictions, a person must not install, use, maintain or attach a tracking device to determine the geographical location:<sup>213</sup>

- of a person, without that person's consent; or

<sup>208</sup> See further [5.158] ff and [5.196]–[5.197] above.

<sup>209</sup> *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). With the exception of South Australia, a 'party' includes a person who overhears, listens to, monitors, or records a private conversation or activity with consent. In South Australia, 'party' is not defined.

<sup>210</sup> *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 to people who would be a 'principal party' to a private conversation or private activity): see also [5.245] ff below.

<sup>211</sup> See [5.198] ff above and Rec 5-3 below.

<sup>212</sup> See [5.168]–[5.169], [5.176] and [5.200] above.

<sup>213</sup> *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).

- of an object or thing, without the consent of a person who is in lawful possession or has lawful control of that object or thing.<sup>214</sup>

5.213 In South Australia, for a vehicle or an object, the prohibition applies ‘without the ... consent of the owner, or a person in lawful possession or lawful control’ of that vehicle or object.<sup>215</sup>

5.214 Like other jurisdictions, the draft Bill provides that a person must not use, install or maintain a tracking device to find, monitor or record the geographical location of an individual without the individual’s consent.

5.215 In relation to the geographical location of a vehicle or other thing, the draft Bill provides that a person must not use, install or maintain a tracking device unless they have the consent of each person who owns, or is in lawful control of, the vehicle or thing.

5.216 The owner of a vehicle or other thing has a proprietary interest in it, even when it is not in their physical possession or control. For that reason, an owner has an interest in whether or not a tracking device is used, installed or maintained in relation to their vehicle or thing.

5.217 Where a vehicle or other thing is the subject of a lease or hire agreement (or other similar agreement), it might be unrealistic to require the owner’s consent each time a person seeks to use, install or maintain a tracking device in relation to a vehicle or thing. Additionally, a person who leases or hires a vehicle or other thing from another person would generally (and particularly where there is a long-term agreement) consider themselves to be in a similar position to an owner for the purpose of giving consent to the use of a tracking device.

5.218 For those reasons, the draft Bill provides that a reference to a person who ‘owns’ a vehicle or other thing does not include a person (an ‘excluded owner’) who owns the vehicle or other thing if:

- another person has the use or control of the vehicle or other thing under a credit agreement, hiring agreement, hire-purchase agreement, leasing agreement or another similar agreement; and
- under the agreement, the excluded owner is not entitled to immediate possession of the vehicle or other thing.

5.219 The draft Bill also requires the consent of each person who is in lawful control of the vehicle or other thing. A person who is in ‘lawful control’ of a vehicle or other thing may include a person who:

<sup>214</sup> In Western Australia, the legislation refers only to a person ‘in possession or having control’ of an object, and does not expressly require that the possession or control be lawful. In the Northern Territory, it was explained that the requirement for the consent of the person who has lawful possession to track a vehicle or thing is to ensure that, ‘for example, transport and taxi companies can use these devices to determine the location of the company vehicle at all times’: Explanatory Statement, Surveillance Devices Bill 2007 (NT) 5.

<sup>215</sup> *Surveillance Devices Act 2016* (SA) s 7(1). If the consent of an owner only is required for the use of a tracking device on a vehicle or other thing, this might enable a person to track a vehicle or thing whilst it is being used by another person, and effectively to track that other person’s location without their knowledge or consent.

- owns a vehicle or other thing;
- leases a vehicle or other thing from another person;
- hires a vehicle or other thing from another person under a hire-purchase agreement;
- borrows a vehicle or other thing from another person; particularly if, for example, the agreement to borrow it was in writing, for a defined period of time or included a requirement for payment.

5.220 In many cases, the owner of a vehicle or thing will also be the person in lawful control of it, for example, where the owner of a car is also the person who drives it. In other cases, these may be different people.

5.221 Tracking a person's vehicle or other thing that is in a person's control is an interference with their privacy. Generally, the person in lawful control of a vehicle or other thing that is being tracked is the person who would be most likely to be affected by that tracking of the vehicle or other thing. Therefore, it is appropriate for that person to give or refuse consent to the use, installation or maintenance of a tracking device.

5.222 In summary, the draft Bill prohibits the use, installation or maintenance of a tracking device to find, monitor or record the geographical location of a vehicle or other thing without the consent of each owner (other than an owner who is excluded), and each person in lawful control of the vehicle or thing.

5.223 Where there is more than one person who is an owner or a person in lawful control, the consent of each person will be required. It is not intended that either the owner or the person in lawful control of a vehicle or other thing can consent to the use, installation or maintenance of a tracking device. This is because, where the owner and the person in lawful control are different people, that approach might enable an owner to consent to the use of a tracking device on a vehicle or thing without the knowledge of the person in lawful control of it.

5.224 The Commission considers that this is a clear and practical approach to the use prohibition for tracking devices. Generally, it will be possible for the user of a tracking device to identify the persons who own or are in lawful control of a vehicle or other thing and, for the reasons previously given, it is reasonable to provide that the device cannot be used without their consent.

### **Data surveillance devices**

5.225 In New South Wales and South Australia, the use, installation or maintenance of a data surveillance device does not require the consent of the user of the computer. Rather, a person must not use, install, maintain or attach a data surveillance device:<sup>216</sup>

---

<sup>216</sup> *Surveillance Devices Act 2007* (NSW) s 10(1); *Surveillance Devices Act 2016* (SA) s 8(1). As the 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 consent.



- in New South Wales—on or in premises, in relation to a computer on those premises, if that involves entry onto or into the premises without the consent of the owner or occupier of the premises, or interference with the computer or a computer network on the premises without the consent of the person in lawful possession or lawful control of the computer or computer network; and
- in South Australia—without the consent of the owner, or the person with lawful control or management, of the computer.

5.226 In the Northern Territory and Victoria, the prohibitions are limited in their application to the use of a data surveillance device by law enforcement officers. It is an offence for those officers to use, install, maintain or attach a data surveillance device without the express or implied consent of the person on whose behalf information is being input into or output from the computer.<sup>217</sup>

5.227 The draft Bill prohibits the use, installation or maintenance of a data surveillance device without the consent of each person who owns, or is in lawful control of, the computer.

5.228 An owner of a computer has a proprietary interest in that computer. An owner also has an interest in the computer when it is not in their possession or control, to the extent that their information is stored on the computer and use of a data surveillance device to access that information would be an interference with their privacy.

5.229 For the same reasons as applied in relation to a tracking device, a reference to a person who ‘owns’ a computer should exclude an owner in circumstances where another person has use or control of the computer under a leasing or other similar agreement, and the owner is not entitled to immediate possession of the computer.<sup>218</sup>

5.230 Further, as is the case for a tracking device, the use of a data surveillance device on a computer that is in a person’s lawful control is likely to be an interference with the privacy of that person. It is also appropriate for that person to be able to give or refuse consent for the use, installation or maintenance of the device.

5.231 The Commission appreciates that a person who experiences an interference with their privacy due to the use of a data surveillance device may not be the owner or the person in lawful control of a computer. A person might use a computer without being in lawful control of it, such as at an internet café or library. Alternatively, information about a person might be input into, output from or stored in a computer that is owned or lawfully controlled by someone else.

<sup>217</sup> *Surveillance Devices Act* (NT) s 14(1); *Surveillance Devices Act 1999* (Vic) s 9(1). In the Northern Territory, this also applies to officers from the Independent Commission Against Corruption.

In Victoria, the prohibition applies to a person who ‘knowingly’ installs, uses, maintains or attaches the device. In New South Wales, it applies to a person who ‘knows’ that the installation, use, maintenance or attachment of the device is without consent.

A similar approach was also used in the Northern Territory’s repealed legislation, which prohibited the use of a data surveillance device by any person: *Surveillance Devices Act 2000* (NT) s 5 (repealed).

<sup>218</sup> See [5.215]–[5.224] above.

5.232 The Commission considered whether this use prohibition could more accurately target a person experiencing an interference with their privacy, for example, a prohibition on the use of a data surveillance device without the consent of the user of the computer, or the person about whom information is input into, output from or stored in the computer. Those options are more precise, but still might not always have the result that consent comes from the person experiencing an interference with their privacy. Additionally, it may be impractical and onerous to apply the provisions in this way, including because it might be difficult to identify each user of a computer (in particular, a public computer) or each person who is the subject of information.

5.233 On balance, the Commission considers that the clearest and most practical approach is to prohibit the use of a data surveillance device without the consent of each person who owns, or is in lawful control of, the computer. Generally, it would be their privacy that would be breached if a data surveillance device was used, installed or maintained to obtain information. Where that is not the case, other legislation, such as state and federal information privacy legislation, will provide protection in some cases.

5.234 It is not intended that either an owner or a person in lawful control of a computer can consent to the use of a data surveillance device, because this might enable an owner to give consent without the knowledge of a person in lawful control. This is consistent with the approach taken in relation to the use of a tracking device.

### Criminal penalty

5.235 The maximum penalty for a contravention of the prohibition on the use of a listening device under the *Invasion of Privacy Act 1971* is imprisonment for two years or 40 penalty units (\$5338).<sup>219</sup> For a corporation, the maximum penalty is 200 penalty units (\$26 690).<sup>220</sup>

5.236 The Commission is of the view that a contravention of each of the use prohibitions under the draft Bill should be a criminal offence, and accordingly a matter for police investigation and prosecution. The Commission does not consider it necessary or desirable to additionally provide for a range of civil penalties. The maximum penalty for the offence should be increased to imprisonment for three years or 60 penalty units (\$8007).

5.237 For corporations, a higher maximum penalty of five times the prescribed maximum will apply by default pursuant to section 181B of the *Penalties and Sentences Act 1992*. Therefore, the maximum penalty for a corporation would be 300 penalty units (\$40 035).<sup>221</sup>

<sup>219</sup> *Invasion of Privacy Act 1971* (Qld) s 43(1). The prescribed value of a penalty unit is currently \$133.45: *Penalties and Sentences Act 1992* (Qld) ss 5(1)(e)(i), 5A(1); *Penalties and Sentences Regulation 2015* (Qld) s 3. For an overview of the maximum penalties in other Australian jurisdictions see [2.39] above.

<sup>220</sup> The *Invasion of Privacy Act 1971* (Qld) 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 the *Penalties and Sentences Act 1992* (Qld) s 181B.

<sup>221</sup> As to corporate officer liability, see [7.52] ff below.

## EXCEPTIONS TO THE USE PROHIBITIONS

5.238 Generally, surveillance devices legislation in other jurisdictions includes specific exceptions that apply to the use of each type of surveillance device. Most exceptions relate to the use of a listening device or an optical surveillance device. There are only limited exceptions that permit the use of a tracking device or a data surveillance device.<sup>222</sup>

5.239 The draft Bill includes a number of exceptions which provide that the use, installation or maintenance of a surveillance device without consent in particular circumstances is not an offence.<sup>223</sup>

5.240 Each exception applies to each category of surveillance device. In principle, the circumstances that form the basis of each exception are equally relevant to each category of surveillance device.

5.241 Generally, the exceptions are in broad terms and their application will depend upon the facts and circumstances of a particular matter. Where an exception includes an element of reasonableness, there are particular requirements that must be satisfied.

5.242 Accordingly, the draft Bill includes exceptions to the use prohibitions, which provide that it is not an offence for a person to use, install or maintain a listening device, an optical surveillance device, a tracking device or a data surveillance device without consent where it is:<sup>224</sup>

- reasonably necessary for the protection of lawful interests;
- reasonably necessary in the public interest;
- to obtain evidence of or information about a serious threat to the life, health, safety or wellbeing of an individual, or of substantial damage to property, if the person believed on reasonable grounds that it was necessary to use the device immediately to obtain the evidence or information;
- to locate or retrieve a vehicle or other thing that has been lost or stolen;
- authorised under another Act of the State or Commonwealth; or
- in prescribed circumstances.

5.243 The Commission considers that these six exceptions in the draft Bill sufficiently provide for the circumstances in which the use, installation or maintenance of a surveillance device without consent might be justified.

---

<sup>222</sup> See Tables 2 and 3 in Appendix C.

<sup>223</sup> Depending on the circumstances, other offences may be relevant: see [D.32]–[D.45] below. It is a defence to a charge under the Criminal Code (Qld) s 408E (Computer hacking or misuse) to prove that a person's use of a restricted computer without the consent of the computer's controller was authorised, justified or excused by law.

<sup>224</sup> The use of a surveillance device with consent and the use of a surveillance device that is unintentional are not included here, because they have been addressed in the draft Bill and the report by other means: see [5.204] ff and [5.117] ff, respectively, above.

5.244 In some instances, the use of a surveillance device may fall within the scope of multiple exceptions. For example, if a person is the victim of a criminal offence, exceptions for the use of a surveillance device in the public interest or to protect a person's safety and wellbeing might apply, if the requirements of the particular exception are met.

## Participant monitoring

5.245 Participant monitoring is permitted in Queensland, the Northern Territory and Victoria. In Queensland, the *Invasion of Privacy Act 1971* provides that the use prohibition for a listening device does not apply 'where the person using the listening device is a party to the private conversation'.<sup>225</sup> In the Northern Territory and Victoria, a person who installs, uses or maintains a listening device or an optical surveillance device to listen to, observe, monitor or record a private conversation or a private activity to which they are a party is not required to inform the other parties or obtain their consent.<sup>226</sup>

5.246 Participant monitoring is prohibited in other jurisdictions, because a person may not record a private conversation or activity to which they are a party without the consent of the other parties.<sup>227</sup> There are, however, some limited legislative exceptions, including the use of a device in a person's lawful interests, in the public interest or for a person's safety or wellbeing.<sup>228</sup>

5.247 Consistently with the Commission's preliminary view,<sup>229</sup> the draft Bill does not include a general exception that permits the use of a listening device or an optical surveillance device for the purpose of participant monitoring.

5.248 As previously explained, this approach is consistent with surveillance devices legislation in several jurisdictions, the Commonwealth law regulating telecommunications, and the general position taken by other law reform bodies and inquiries that have considered this issue.<sup>230</sup> It also takes into account advances in technology, which have increased the accessibility and capabilities of surveillance devices and therefore the ability of individuals to engage in participant monitoring.

<sup>225</sup> *Invasion of Privacy Act 1971* (Qld) s 43(2)(a).

<sup>226</sup> *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).

<sup>227</sup> *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. That offence also does not include a participant monitoring exception: ALRC Report No 123 (2014) [14.53].

<sup>228</sup> As to the exceptions, see [5.254] ff, [5.283] ff and [5.323] ff below. See also ACT Review (2016) [6.9]–[6.11]; NSWLRC Interim Report No 98 (2001) [2.99]; VLRC Consultation Paper No 7 (2009) [5.21], [6.132] ff; VLRC Report No 18 (2010) [6.54], [6.59]–[6.69]; NZLC Report No 113 (2010) [3.80] ff.

<sup>229</sup> QLRC Consultation Paper No 77 (2018) [3.98]–[3.105].

<sup>230</sup> See the discussion of civil surveillance law reform reviews in Appendix E.

5.249 This approach is also consistent with the Commission's adoption of a consent-based approach to the regulation of surveillance devices, which generally prohibits the use of a surveillance device, without consent, unless an exception applies.<sup>231</sup> Although the adoption of that model—and the consequent prohibition of participant monitoring—is a significant departure from the current scheme of regulation, the Commission has concluded that it is necessary and appropriate in all of the circumstances.

5.250 In some circumstances, it may be appropriate for a person who is or is not a party to a private conversation or a private activity to record it without consent, for example, if a person is being threatened with or experiencing domestic violence.

5.251 However, as a matter of principle, the mere fact that a person is a party to a conversation or activity should not automatically permit the use of a surveillance device, and the consequent interference with the privacy of another party. Rather, the use of a surveillance device without the consent of the other parties should be permitted only if there are particular reasons that justify interference with a person's privacy.

5.252 Circumstances in which the use of a surveillance device would be justified can be addressed in a way that balances considerations of individual privacy against the need to use a device without consent in limited circumstances, by including specific exceptions in the draft Bill.

5.253 A number of relevant exceptions, including use of a surveillance device where it is in a person's lawful interests, in the public interest or relevant to considerations of safety and wellbeing, are discussed below.

## Protection of lawful interests

5.254 In jurisdictions where surveillance devices legislation does not include a general exception permitting participant monitoring, a party to a private conversation or a private activity may use a listening device or an optical surveillance device to record that conversation or activity if it is reasonably necessary for the protection of their lawful interests.<sup>232</sup> Where this exception applies, a party can record a conversation or activity without the consent of the other parties.

5.255 Specifically, this exception applies in relation to listening devices in the Australian Capital Territory, New South Wales, South Australia, Tasmania and Western Australia, and to optical surveillance devices in Western Australia.<sup>233</sup>

<sup>231</sup> See [5.204] ff above.

<sup>232</sup> *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.

<sup>233</sup> Optical surveillance devices are also regulated in New South Wales and South Australia. 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). The position in South Australia is discussed separately below.

5.256 Except in South Australia, a party may record a private conversation or activity with the consent of a principal party<sup>234</sup>—that is, a person who is speaking or being spoken to or participating in an activity—if it is reasonably necessary to protect that principal party’s lawful interests.<sup>235</sup> As a result, a recording may be made by a principal party without the consent of others (in this case, 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.

5.257 This may be illustrated by the following scenario. If A and B have a private conversation, they are both principal parties. If A considers that it is reasonably necessary to protect A’s lawful interests, A may record the conversation without the consent of B. If C is permitted to listen to that conversation, C could record the conversation with A’s consent and to protect A’s lawful interests without the consent of B.

5.258 In those jurisdictions, an exception permitting the use of a listening device or an optical surveillance device in a person’s lawful interests operates as a limited form of participant monitoring, but does not extend to their use by a person who is not a party.

5.259 In South Australia, a party to a private conversation may use a listening device to record the conversation, if that is reasonably necessary for the protection of the lawful interests of that person.<sup>236</sup> In addition, a person may install, use or maintain:<sup>237</sup>

- 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 of the premises or vehicle, or some other person; or
- an optical surveillance device on premises without fulfilling the requirements for consent, if the use of the device is reasonably necessary for the protection of the lawful interests of that person.<sup>238</sup>

5.260 Some reviews and inquiries have recommended that an exception about lawful interests should operate objectively, considering whether surveillance was ‘necessary and proportionate’ and balancing ‘lawful interests’ against other relevant

<sup>234</sup> See [5.196] ff above as to parties. In these jurisdictions, in relation to private conversations, a ‘principal party’ is a person who is speaking or being spoken to. A ‘party’ to a conversation is a person who is a principal party, or another person who listens to or records the conversation with consent. In Western Australia, in relation to optical surveillance devices, these definitions also include, respectively, a person who participates in a private activity and a person who observes or records that activity with consent.

<sup>235</sup> 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.

<sup>236</sup> The term ‘party’ is not defined. Here, the consent of a principal party is not required.

<sup>237</sup> *Surveillance Devices Act 2016* (SA) ss 4(2)(a)(ii), 4(2)(c), 5(4)(b). As to the definition of ‘premises’, see n 191 above. As to the use of a device by an investigation agent or loss adjuster, see [5.354] ff below.

<sup>238</sup> Generally, a person who installs, uses or maintains an optical surveillance device must not do so without consent from the parties and the owner or occupier of the premises, vehicle or thing: see [5.185] above.

interests, including the protection of personal privacy.<sup>239</sup> Others have observed that an exception about lawful interests is potentially uncertain and broad, and that the use of a surveillance device in these circumstances requires greater regulation.<sup>240</sup>

### ***The meaning of ‘lawful interests’***

5.261 The term ‘lawful interests’ is not defined by surveillance devices legislation, but has been the subject of judicial consideration.

5.262 In *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd*, Doyle J reviewed relevant decisions and stated that ‘the concept of “lawful interests” is of uncertain content’ and that, whilst there are some general propositions and guidance in the relevant authorities, whether a recording was made to protect a person’s lawful interests ‘remains ... very much anchored in the facts of the particular case’.<sup>241</sup> He stated that:<sup>242</sup>

Based on my survey of the authorities, it would appear that a recording made merely pursuant to a practice of doing so, for the purpose of having a reliable record or in case it turns out to be advantageous in some future setting is not enough to warrant its characterisation as a recording made to protect the person’s lawful interests. Further, this will generally be so even if the recording occurs in a commercial setting where a person’s business or legal interests are the subject of discussion, and may still be so even where the person making the recording has concerns about the honesty or conduct of the other party to the conversation, is in dispute with that party or is contemplating proceedings against that party. In *Violi v Berrivale Orchards Ltd*, the fact that the parties were in a contractual dispute and that one party feared the other might not tell the truth was not enough; in *Thomas v Nash*, the contemplation of future litigation was not enough; and in *RRG Nominees Pty Ltd v Temporary Fencing Australia Pty Ltd (No 3)*, the existence of concerns about the conduct of another in their commercial dealings was not enough.

In summary, while a threat to a person’s physical safety, or the desire to uncover a crime or resist an allegation of crime, will often give rise to a lawful interest that would warrant protection through the use of a listening device, not every

<sup>239</sup> ACT Review (2016) [6.15]; SA Legislative Review Committee Report (2013) 38, which considered the Surveillance Devices Bill 2012 (SA) (not passed). See also VLRC Report No 18 (2010) [6.78]–[6.79]; QLRC Consultation Paper No 77 (2018) [3.116]–[3.119].

<sup>240</sup> See, eg, NSWLRC Interim Report No 98 (2001) [2.102], [2.104]; ALRC Report No 22 (1983) vol 2, [1130], [1135]. See also QLRC Consultation Paper No 77 (2018) [3.95]–[3.96].

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: NSWLRC Interim Report No 98 (2001) [2.102], note 149. See also QLRC Consultation Paper No 77 (2018) [3.97], [D.7]–[D.8].

<sup>241</sup> (2018) 132 SASR 63, 94 [101]. It was also observed that decisions ‘are not all easy to reconcile’ and that this is partly ‘a reflection of the case and fact specific nature of the concept of lawful interests’: at 90 [96]. See also, generally, *D-P v Minister for Child Protection* (2018) 132 SASR 102, 116–18 [69]–[74] (Parker J); and *Thomas v Nash* (2010) 107 SASR 309, 317 [47]–[48] (Doyle CJ). See generally, H Douglas and M Burdon, ‘Legal responses to non-consensual smartphone recordings in the context of domestic and family violence’ (2018) 41(1) *University of New South Wales Law Journal* 157, 174 ff.

<sup>242</sup> *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd* (2018) 132 SASR 63, 95 [103]–[105].

See also, as to the points made by Doyle J in his survey of authorities, *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, 586–7 [27]–[33] (Branson J); *Thomas v Nash* (2010) 107 SASR 309, 317 [46]–[49] (Doyle CJ); *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [31] (White J).

commercial or legal interest, or dispute in relation to such an interest, will suffice to establish a lawful interest for the purposes of the legislation.

However, it would seem that where a dispute has arisen, and has crystallised into a real and identifiable concern about the imminent potential for significant harm to the commercial or legal interests of a person, this may suffice to give rise to lawful interests warranting protection through the use of a listening device. This was so in *Chao v Chao* and *Metz Holdings Pty Ltd v Simmac Pty Ltd (No 1)*. It was also so in *Dong v Song*, where [it was considered] critical that the situation had moved from a general or abstract concern to have a reliable record in the hope it might later be of some advantage, into a particular concern about the honesty of the defendants and the significance of the relevant conversation to imminent legal proceedings.

5.263 Some circumstances in which a person has been found to have used a surveillance device in a way that protected their lawful interests include:<sup>243</sup>

- a dispute about property arrangements, which included threats of ejection from the property, where litigation had already commenced;
- a dispute concerning legal obligations arising under a sale agreement between the parties;
- a ‘serious dispute’ about misleading and deceptive conduct related to the purchase of a business, where legal proceedings were imminent;
- current or continuing abuse and exploitation, contravention of a domestic violence order where the person had a ‘genuine concern for their own safety’, or more generally, where the circumstances involved a ‘serious crime’; or
- to prevent or refute accusations that a person had fabricated a relevant conversation, particularly in the context of a criminal investigation.

5.264 In contrast, circumstances in which a person was found to have used a surveillance device in a way that did not fall within the exception for protection of their lawful interests include:<sup>244</sup>

- a recording made in case it turned out to be advantageous in the future (including where there was contemplation of future litigation), or pursuant to a ‘usual practice’ where there was no anticipated or actual dispute;
- a recording that was not made to *protect* a lawful interest, namely, where a recording was made to ‘trap’ the other party into engaging in particular

<sup>243</sup> See generally *R v Le* (2004) 60 NSWLR 108, 124 [79] (Hulme J), 124–6 [83]–[85] (Adams J); *Chao v Chao* [2008] NSWSC 584, [8]–[9]; *Metz Holdings Pty Ltd v Simmac Pty Ltd* (2011) 193 FCR 195, 196 [1]–[2], 199 [23]–[24] (and see *Metz Holdings Pty Ltd v Simmac Pty Ltd (No 2)* (2011) 216 IR 116, 145, [159]–[160]); *DW v The Queen* (2014) 239 A Crim R 192, 199 [37], 201–02 [47]–[50]; *Groom v Police (SA)* (2015) 252 A Crim R 332, 342–3 [37]–[43]; *Dong v Song* (2018) 331 FLR 326, 335–6 [44]–[49]; *R v Coutts* [2013] SADC 50, [26]. See also Explanatory Memorandum, Listening Devices Bill 1992 (ACT) 2; *Alliance Craton Explorer Pty Ltd v Quasar Resources Ltd* [2010] SASC 266; *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, 587 [31]–[32].

<sup>244</sup> See generally *Sepulveda v The Queen* (2006) 167 A Crim R 108, 134 [130]–[131], 136–7 [137]–[144]; *Thomas v Nash* (2010) 107 SASR 309, 317 [44]–[50]; *Georgiou Building Pty Ltd v Perrinepod Pty Ltd* [2012] WASC 72 (S), [17]; *Levy v Bablis* [2013] NSWCA 28, [109]; *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [26]–[33].



conduct where the ‘threat of disclosure’ of the recording could be used to ‘persuade’ the other party to take certain action; or

- a victim of crime recording a conversation with an alleged offender for the purpose of obtaining admissions; however, this will depend on the particular circumstances, including the proximity in time of the offending to the conversation and the victim’s ability to take other reasonable action, such as approaching the police.<sup>245</sup>

5.265 In *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd*, Doyle J’s reasoning also highlighted the importance of the phrase ‘protection of’ lawful interests. He concluded that, whilst there were relevant ‘contemplated, and then actual, legal proceedings’, some recordings were made with a view to advancing those proceedings or obtaining evidence to use in the proceedings (rather than for the protection of the plaintiff’s commercial interests at the time when they were in jeopardy). Those were held not to be recordings made ‘for the protection’ of the plaintiff’s lawful interests.<sup>246</sup>

5.266 In *Sepulveda v The Queen*, the New South Wales Court of Criminal Appeal stated that this 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’.<sup>247</sup> 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. It has been explained that the question of reasonable necessity should be judged

<sup>245</sup> See, in particular, *Sepulveda v The Queen* (2006) 167 A Crim R 108. In that case, the appellant had been convicted of historical sexual offences. One of the complainants in those offences had, without the appellant’s knowledge and approximately 15 to 20 years after the offending occurred, recorded a conversation between himself and the appellant in which the appellant made admissions. The New South Wales Court of Appeal held that the making of the recording was not ‘reasonably necessary’, because the complainant could have approached the police with his complaint rather than moving directly to recording a conversation himself. It also observed that the term ‘lawful interests’ should not be construed as having an open ended meaning, noting that a broad interpretation could leave open ‘the covert recording of a conversation by any person who alleges [they are] a victim of crime, and who speaks to the alleged offender for the purpose of obtaining admissions’. Such an approach could serve to undermine the legislation’s purpose of protecting privacy. See further [5.266]–[5.267] below.

Cf *DW v The Queen* (2014) 239 A Crim R 192, in which it was held that a recording made by a child complainant of a conversation with the alleged perpetrator was made for the protection of the complainant’s lawful interests (at 202 [50]–[51] (Ward JA; Harrison and RA Hulme JJ agreeing)):

In *Sepulveda*, the recording was made by an adult, some years after the alleged assaults. Here, it was made by a [14 year old] child and it was made while the assaults were ongoing. The recording was made prior to any investigation by the police of allegations of sexual misconduct by the appellant. ... [T]he complainant was frightened of the appellant, with whom she was living, as a result of his violent behaviour and ... the only other adult in the house had been convinced by the appellant that she was lying. ... [I]t was not practicable in the circumstances ... for the complainant to contact police in order to seek to arrange a warrant to record conversations with her father.

<sup>246</sup> (2018) 132 SASR 63, 97 [114]–[116].

<sup>247</sup> (2006) 167 A Crim R 108, 136 [142] and see 131–2 [115]. See also *Thomas v Nash* (2010) 107 SASR 309, 317 [49]; *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [29]; *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd* (2018) 132 SASR 63, 94–5 [102]. In *Nanosecond Corporation* it was stated that ‘the exception in relation to “lawful interests” should not be construed so widely as to undermine the protection intended to [be] afforded to private conversations’. The VLRC stated that the court in *Sepulveda* interpreted the phrase ‘reasonably necessary for the protection of the lawful interests’ of a principal party ‘narrowly, in order to prevent the exception from swallowing the rule’: VLRC Report No 18 (2010) [6.62].

objectively and based upon the circumstances existing at the time of recording, taking into account:<sup>248</sup>

- 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.

5.267 The term ‘reasonably necessary’ has been held to mean reasonably ‘appropriate, but not essential’, for the protection of the lawful interests of the person. Further, the ordinary meaning of ‘protection’ as ‘shelter, defence, or preservation from harm, danger, or evil’ has been said to be apt in this context.<sup>249</sup>

### ***The Commission’s view***

5.268 The draft Bill does not provide a general exception that permits participant monitoring of private conversations or private activities.<sup>250</sup> There must be some other justification to allow a party to use a surveillance device without the consent of the other parties to the conversation or activity.

5.269 Accordingly, the draft Bill contains a limited, specific exception which provides that it is not an offence for a person to use, install or maintain a surveillance device without consent if use of the device is ‘reasonably necessary to protect the lawful interests’ of a person.

5.270 The draft Bill does not define the term ‘lawful interests’. However, there is an established line of judicial reasoning interpreting the meaning of that term, and whether the test will be met in the particular circumstances of each case. Additionally, it is beneficial that there is scope for the concept of lawful interests to be considered on the facts of each case.

5.271 The inclusion of the requirement that the use is ‘reasonably necessary’ and ‘to protect’ a person’s lawful interests limits the scope of the exception. In particular,

<sup>248</sup> *Sepulveda v The Queen* (2006) 167 A Crim R 108, 132 [116]–[118], 136–7 [138]–[139], [142]; *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, 585 [23], 587 [32]; *Marsden v Amalgamated Television Services Pty Ltd* [2000] NSWSC 465, [14], [17]–[18], [20]–[23]; *Georgiou Building Pty Ltd v Perrinepod Pty Ltd* [2012] WASC 72 (S) [16]–[17]; *RRG Nominees Pty Ltd v Visible Temporary Fencing Australia Pty Ltd (No 3)* [2018] FCA 404, [29].

See also ACT Review (2016) [6.14]–[6.15], where it was explained that by applying this approach:

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.

It is not sufficient that a person who uses a surveillance device ‘believed it to be reasonably necessary to protect a lawful interest’: VLRC Report No 18 (2010) [6.65].

<sup>249</sup> *Sepulveda v The Queen* (2006) 167 A Crim R 108, 132 [117], [120]; *Georgiou Building Pty Ltd v Perrinepod Pty Ltd* [2012] WASC 72 (S) [16]. In *Georgiou*, it was explained that the word ‘necessary’ should, in this context, be construed as meaning ‘appropriate, but not essential or unavoidable’.

<sup>250</sup> See [5.247] ff above.

the phrase 'reasonably necessary' has been explained as requiring an objective test, based upon circumstances existing at the time of the use of the device and taking into account relevant factors. It is important that this exception incorporates the concept of reasonableness as an objective test, so that it operates in appropriate circumstances.

5.272 This exception should apply to any person who can establish that they hold a lawful interest, and that the use of a surveillance device is reasonably necessary for the protection of that lawful interest.

5.273 Whether or not the use of a surveillance device is permitted should not turn on a person's status or role in a particular situation, but rather on their reasons for using a surveillance device. A person who is a party to a conversation or activity might have a lawful interest in it. Equally, a person who does not have any involvement in a situation could nonetheless hold a relevant lawful interest. For example, a person might overhear a conversation that is between other people but of relevance to their own lawful interests, such as a conversation about a legal dispute in which they are a defendant. Additionally, involvement in a situation is of less relevance to the use of a tracking device or a data surveillance device.

5.274 A person who establishes that they have a lawful interest, and that it is reasonably necessary to protect it by using a surveillance device, has a reason justifying the use of a surveillance device. Use in those circumstances should not be limited only to a particular category of people. Accordingly, the draft Bill provides that it is not an offence for a person to use, install or maintain a surveillance device where use of the device is reasonably necessary for the protection of their lawful interests.

5.275 The Commission also notes that it might be useful for the new regulator to provide guidelines about this exception, including examples of circumstances in which the use of a surveillance device might be reasonably necessary to protect a person's lawful interests.<sup>251</sup>

### ***The lawful interests of other people***

5.276 The draft Bill provides that it is not an offence for a person to use, install or maintain a surveillance device where use of the device is reasonably necessary to protect their own lawful interests. It also provides that it is not an offence for a person to use a surveillance device to protect another person's lawful interests, when authorised to use the surveillance device on behalf of that other person.

5.277 Surveillance devices legislation in some other jurisdictions recognises the use of a surveillance device on another person's behalf, by prohibiting a person from

---

251

As to the regulator's power to make guidelines, see [10.109] ff and Rec 10-10(d) below.

causing or permitting a surveillance device to be used,<sup>252</sup> or by including in some exceptions use that is on behalf of another person.<sup>253</sup>

5.278 More specifically, exceptions for use of a surveillance device to protect a lawful interest often permit a party to record a private conversation or private activity if it is with the consent of a principal party and is reasonably necessary to protect that principal party's lawful interests. In South Australia, a listening device may sometimes also be used to protect another person's lawful interests.<sup>254</sup>

5.279 The Commission notes that, in circumstances where another person caused or permitted the unlawful use, installation or maintenance of a surveillance device, the provisions of the Criminal Code relevant to charging and convicting principal offenders may apply. Those persons can be deemed to have taken part in committing the offence, and can be charged with and found guilty of the offence.<sup>255</sup>

5.280 Generally, a person can appoint another person as their agent, so that the agent acts as the representative of the person.<sup>256</sup> This will generally be sufficient for the appointment of an agent to use a surveillance device in some circumstances, such as where a conversation is recorded by an agent and with the consent of the other parties.

5.281 However, unlike other exceptions included in the draft Bill, this exception is framed in terms of the particular interests of the person using the device.<sup>257</sup> The law of agency could operate to effectively satisfy this requirement, but for clarity and because the use of a surveillance device can be an offence, the use of a device by one person in another person's lawful interests should be the subject of an express provision.

5.282 Accordingly, the draft Bill provides that it is not an offence for a person to use, install or maintain a surveillance device on behalf of another person who has authorised the person to use the device on that other person's behalf, where the use is reasonably necessary for the protection of the lawful interests of that other person. The draft Bill does not provide that a person may use a device for that purpose on their own initiative, because the scope of the exception would then be too broad to adequately regulate the use of a surveillance device.

<sup>252</sup> *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). The use prohibitions that include the concepts of 'cause' and 'permit' are limited to listening devices, except in Western Australia where the legislation extends to causing any device to be used, installed, maintained or attached.

<sup>253</sup> *Listening Devices Act 1992* (ACT) s 4(3); *Surveillance Devices Act 1998* (WA) ss 5(2)(d), (3), 6(2)(d), (3), 26(1)–(2), 27(1)–(2). In Western Australia, some provisions refer more specifically to 'a person who is acting on behalf of a party' to a private conversation or a private activity: ss 26(2), 27(2).

<sup>254</sup> See [5.259] above.

<sup>255</sup> Criminal Code (Qld) s 7; see also n 158 above.

<sup>256</sup> See generally, LexisNexis Australia, *Halsbury's Laws of Australia* (at 14 July 2014) 15 Agency.

<sup>257</sup> Cf, eg, the exceptions to the use prohibitions which provide that it is not an offence for any person to use a device in circumstances where it is reasonably necessary in the public interest, or where it is to obtain evidence or information in relation to a serious threat to an individual's life, health, safety or wellbeing, or of substantial damage to property: see [5.283] ff below.

## Public interest

5.283 In Western Australia and the Northern Territory, the term ‘public interest’ is defined by surveillance devices legislation to include:<sup>258</sup>

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.

5.284 The term ‘public interest’ is used in diverse contexts and is generally interpreted broadly. What is ‘in the public interest’ depends on the context, circumstances and purpose, but it does not include circumstances that are ‘merely of interest’ to the public.<sup>259</sup>

5.285 Some concepts that might inform a general understanding of the term ‘public interest’ are that the relevant matters or interests being considered ‘convey a sense of matters of public concern ... as opposed to matters that are the concern of a particular person or entity’, or that there are social values that should be protected. Within various approaches, one constant feature of a public interest test is that the meaning of the term is decided in context and in a way that ‘balances’ various interests to ensure ‘that recognition of the prevailing public interest goes only as far as is necessary, with the least possible (‘proportionate’) compromising of another interest’.<sup>260</sup>

5.286 The public interest might intersect with an individual’s interest, if the general application of that individual’s interest would affect others in a similar way. For example, the NSWLRC observed that ‘a person’s interest in preventing unjustified intrusions into his or her personal privacy, or protecting the right to a fair trial, are classic examples of private interests which it is in the public interest to uphold’.<sup>261</sup>

5.287 In general terms, examples of matters that might, depending on the circumstances, be ‘in the public interest’ include:<sup>262</sup>

<sup>258</sup> *Surveillance Devices Act* (NT) s 41; *Surveillance Devices Act 1998* (WA) s 24 (definition of ‘public interest’). In the Northern Territory, the scope of the legislation is restricted to emergency use in the public interest: pt 6. See further [5.289] below.

<sup>259</sup> S Rice, ‘The meaning(s) of public interest in law’ in B Douglas and J Wodak (eds), *Who speaks for and protects the public interest in Australia? Essays by notable Australians* (2015) 24, 24; SA Legislative Review Committee Report (2013) 38, 74; ACT Review (2016) [6.18].

<sup>260</sup> See Rice, above n 259, 24–5.

See also NSWLRC Interim Report No 98 (2001) [6.4] ff; SA Legislative Review Committee Report (2013) 38; VLRC, Report No 18 (2010) [7.187]; ALRC Discussion Paper No 80 (2014) [8.36]–[8.37].

<sup>261</sup> NSWLRC Interim Report No 98 (2001) [6.7]. See also NSWLRC Report No 108 (2005) [5.15]; SA Legislative Review Committee Report (2013) 38, 74; Privacy Committee of South Australia, *Responses to questions on notice from the South Australian Legislative Review Committee: Inquiry into surveillance devices* (2013) 2; ACT Review (2016) [6.18]. See also ALRC Discussion Paper No 80 (2014) [2.12].

<sup>262</sup> NSWLRC Interim Report No 98 (2001) [6.5], [6.11]; NSWLRC Report No 108 (2005) [5.21]; SA Legislative Review Committee Report (2013) 38–39, 76; Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (September 2016) 6–7.

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.

- the prevention and detection of illegal activities, for example, the investigation of a crime or detection of insurance fraud;
- public officer maladministration in relation to performing official functions, for example, the unauthorised use of public funds, corruption or bribery;
- national security;
- conduct causing a substantial risk to public health, safety, or the environment;
- the protection of public assets;
- retail practices that contravene consumer protection laws; and
- the prevention of wrongful prosecutions.

5.288 The ALRC has observed that because community expectations of privacy change over time, it is preferable to provide a non-exhaustive list of matters that are in the public interest than to define the term 'public interest'. The ALRC stated that this would 'allow the meaning of public interest to develop in line with changing community attitudes and developments in technology'.<sup>263</sup>

### ***Surveillance devices legislation in other jurisdictions***

5.289 In Western Australia and the Northern Territory, the term 'public interest' is defined, as explained in [5.283] above. The provisions permit the use of a listening device or an optical surveillance device to listen to, observe, monitor or record a private conversation or activity:<sup>264</sup>

- by a party or a person acting on their behalf, if a principal party consents and there are reasonable grounds for believing that the use of the device is in the public interest (Western Australia);<sup>265</sup>
- by a person on behalf of a child or protected person under their care, supervision or authority 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 (Western Australia);<sup>266</sup>
- 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

<sup>263</sup> ALRC Report No 123 (2014), [8.39]; see also Rice, above n 259, 25.

<sup>264</sup> These provisions do not apply if, in the course of installing or using a device, a person does an act that is unlawful under any other law: *Surveillance Devices Act* (NT) s 42; *Surveillance Devices Act 1998* (WA) s 25.

<sup>265</sup> *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(1), (2), 27(1), (2).

<sup>266</sup> *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3). A 'protected person' is a person who, by reason of mental impairment, is unable to consent to the use of a listening device or an optical surveillance device in accordance with the public interest provisions: ss 26(4), 27(4).

the use of the device is in the public interest (an 'emergency use') (Western Australia, Northern Territory).<sup>267</sup>

5.290 In South Australia, the prohibitions against using a listening device or an optical surveillance device do not apply if the use of the device is in the public interest.<sup>268</sup> The term 'public interest' is not defined.

5.291 The ACT Review, noting that this concept is generally interpreted broadly, recommended that legislation 'allow surveillance when it is carried out to protect a public interest and the surveillance activity is necessary and proportionate'.<sup>269</sup> The VLRC decided not to recommend a 'broad public interest exception' because it considered that the scope would be 'too uncertain for use in a regime that contains criminal sanctions'.<sup>270</sup>

### **Alternative approaches**

5.292 The ALRC and the NSWLRC have each proposed an alternative legislative scheme to address the use of a device in the public interest.

5.293 The NSWLRC proposed that covert surveillance should be permitted in the public interest only where it is authorised by an 'appropriate issuing authority',<sup>271</sup> having regard to factors such as:<sup>272</sup>

- the nature of the issue in respect of which the authorisation is sought;
- the public interest (or interests) arising from the circumstances;

<sup>267</sup> *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.

<sup>268</sup> *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 an 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 QLRC Consultation Paper No 77 (2018) [3.106] ff, [3.145] ff.

The communication or publication of information obtained from use of a surveillance device in the public interest is limited to particular circumstances: see [6.95], [6.97]–[6.98] below.

<sup>269</sup> ACT Review (2016) [2.5](d), [6.18], [6.21]. However, it was also recommended that subsequent communication should require a court order, unless the communication is to a media organisation subject to an appropriate code of conduct: see [6.104] below.

<sup>270</sup> VLRC Report No 18 (2010) [6.81]. In a recent New South Wales review about landowner protection from unauthorised filming or surveillance, it was recommended that the *Surveillance Devices Act 2007* (NSW) should be reviewed to consider whether to 'insert a public interest exemption for unauthorised filming or surveillance'. The NSW Government has supported this recommendation in principle, and indicated this it would establish a working group for this purpose: Parliament of NSW Legislative Council, Select Committee on Landowner Protection from Unauthorised Filming or Surveillance, *Landowner Protection from Unauthorised Filming or Surveillance* (October 2018) [3.11]–[3.18], [3.54], Rec 3; N Blair, NSW Government, Response.

<sup>271</sup> 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]–[6.36], Rec 52.

<sup>272</sup> NSWLRC Interim Report No 98 (2001) [6.37]–[6.38], Rec 54, as amended by 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 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;
- 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.

5.294 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’.<sup>273</sup>

5.295 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.<sup>274</sup>

5.296 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’, noting that the activities of the media can offer significant public benefit and might sometimes justify the use of a surveillance device without consent.<sup>275</sup>

5.297 In the ALRC’s view, the proposed 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:<sup>276</sup>

- 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

<sup>273</sup> 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]. See also [6.100]–[6.102] below.

<sup>274</sup> NSWLRC Interim Report No 98 (2001) [6.24]–[6.27].

<sup>275</sup> ALRC Report No 123 (2014) [14.58] ff, Rec 14-5. The ALRC stated that this defence is particularly important if participant monitoring exceptions are not included in legislation.

<sup>276</sup> Ibid [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 [6.103] 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)

### ***The Commission's view***

5.298 The draft Bill provides that it is not an offence for a person to use, install or maintain a surveillance device if use of the device is 'reasonably necessary in the public interest'. This exception is not dependent on the individual interests of the person using the surveillance device.

5.299 Again, it is important that this exception incorporates the concept of reasonableness as an objective test, so that it operates in appropriate circumstances. It is not intended that a person's subjective belief as to whether the use of a surveillance device is in the public interest should inform the circumstances in which use is not an offence.

5.300 The Commission considers that an exception which simply permits the use of a device 'in the public interest' is vague in nature and could result in uncertainty or be open to abuse.

5.301 However, the Commission does not consider that the term 'public interest' should be defined. An understanding of 'public interest' is generally contextual. Relevant public interests and the outcome of balancing various interests will depend upon the facts of a case. What is in the public interest also changes over time.

5.302 There have been rapid technological advances, which have increased access to surveillance devices and the capacity to use those devices for surveillance purposes. More generally, changes in society and to community attitudes have impacted upon expectations of privacy and the understanding of matters that are (or are not) within the public interest. Future changes will also impact on the concept and understanding of the public interest.

5.303 Any definition of 'public interest' that attempted to accommodate this ongoing change might be overly general, and any definition that attempted to more specifically explain the term might be too narrow or inflexible. It is preferable that the term 'public interest' continues to develop in accordance with community attitudes and technology.<sup>277</sup>

5.304 However, it is appropriate that the draft Bill provide guidance about the circumstances in which using a device might be reasonably necessary in the public interest. Drawing upon the alternative approaches suggested by the NSWLRC and the ALRC, the Commission is of the view that this exception should include a list of relevant matters, to provide a framework for courts and persons in determining

---

<sup>277</sup>

See also ALRC Discussion Paper No 80 (2014) [8.38]–[8.39].

whether the use of a surveillance device is reasonably necessary in the public interest in particular circumstances.<sup>278</sup>

5.305 This approach offers a greater degree of certainty about the scope of the exception. It provides guidance about the concept of the public interest, ensures that a person does not rely solely on their own view of what is in the public interest, and facilitates a consistent approach to the operation of the exception whilst allowing the concept of the public interest to develop over time.

5.306 Accordingly, the draft Bill provides that, in considering whether the use of a surveillance device is ‘reasonably necessary in the public interest’, a court must consider the following matters, as they existed when the person used, installed or maintained the device:

- the subject matter of the use of the device;
- the information that the person reasonably expected would be obtained from the use of the device;
- the purpose for which the person intended to use information that the person reasonably expected would be obtained from the use of the device;
- the nature of the public interest that arose in the circumstances;
- whether the public interest could have been served in another reasonable way;
- the extent to which the use, installation or maintenance of the device affected, or was likely to affect, the privacy of an individual; and
- whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

5.307 The focus of this exception is on the public interest at the time of the use, installation or maintenance of the surveillance device. That is, the relevant consideration is whether use of a surveillance device was ‘reasonably necessary in the public interest’, and not ‘whether the information obtained through surveillance was, in hindsight, information in the public interest’.<sup>279</sup> This is reflected in the requirement that the use be ‘reasonably necessary’, and in the matters that have been included.

5.308 For example, in appropriate circumstances, a member of the public might rely on this exception to use a surveillance device to make an audio or audio-visual recording about the commission of a crime to give to police in the course of an investigation into a suspected criminal offence.

---

<sup>278</sup> Unlike the alternative approaches proposed by the NSWLRC and the ALRC, the draft Bill does not include any requirement that the use of a surveillance device be authorised by an authority prior to its use, or provide a defence for the use of a surveillance device in particular circumstances.

<sup>279</sup> ALRC, Report No 123, [14.62].

5.309 It might be useful for the new regulator to provide guidelines about the public interest exception, including examples of circumstances in which the use of a surveillance device might be reasonably necessary in the public interest.<sup>280</sup>

### **Media organisations and journalists**

5.310 An exception for the use, installation or maintenance of a surveillance device where it is reasonably necessary in the public interest may be of particular relevance to media organisations or journalists.

5.311 The public interest in a free press is fundamental to a liberal democracy.<sup>281</sup> The High Court has held that ‘each member of the Australian community has an interest in disseminating and receiving information’ relevant to government and political matters that affect the Australian public.<sup>282</sup> In another decision, the Victorian Court of Appeal held that the public has a ‘right to know’ about matters falling within their legitimate area of interest, and that the media have a ‘right to disseminate information’ to satisfy that right to know.<sup>283</sup>

5.312 However, the public interest in a free press is not absolute. It must be balanced with other countervailing public interests, such as the public interest in the rule of law and in the civil liberties of individuals, including privacy.<sup>284</sup> The Victorian Court of Appeal observed that the public’s ‘right to know’ will assume greater or lesser importance depending on the subject matter of the information being published.<sup>285</sup>

5.313 Media broadcasting codes of practice state that it is necessary to balance the broadcasting of matters that are in the public interest against other matters, including individuals’ right to privacy. The Australian Communications and Media Authority privacy guidelines for broadcasters state that:<sup>286</sup>

The broadcast of personal information or material that invades privacy, without consent, will not breach the [broadcasting codes of practice] if there is a clear

<sup>280</sup> See also NSWLRC Interim Report No 98 (2001) [6.11], in which the NSWLRC made a similar observation. As to the regulator’s power to make guidelines, see [10.109] ff and Rec 10-10(d) below.

<sup>281</sup> The Right Honourable Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, Report (November 2012) vol 1, 56 ff (‘Leveson Inquiry Report’).

<sup>282</sup> *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 570–1. In that case, the High Court also stated that ‘[t]he duty to disseminate such information is simply the correlative of the interest in receiving it’: 571. See also *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211, 264 (McHugh J), in which it was held that ‘the general public has a legitimate interest in receiving information’ about the exercise of public functions and powers.

<sup>283</sup> *News Digital Media v Mokbel* (2010) 30 VR 248, [36] (Warren CJ and Byrne AJA). See also *Victoria v The Australian Building Construction Employees’ and Builders’ Labourers’ Federation* (1982) 152 CLR 26, 98–9 (Mason J), in which it was noted that the importance of the public having access to information which it has a legitimate interest in knowing is of equal importance to freedom of discussion and speech.

<sup>284</sup> Leveson Inquiry Report, above n 281, vol 1, 69 ff.

<sup>285</sup> See, eg, *News Digital Media v Mokbel* (2010) 30 VR 248, [36] (Warren CJ and Byrne AJA), noting that ‘information may, at one end of the spectrum, concern the performance of the functions of those in the highest office; and at the other no more than salacious gossip about personal shortcomings of the less lofty’.

<sup>286</sup> Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (September 2016) 6–7. See also the ABC Code of Practice and Associated Standards (January 2019) [6. Privacy] which states, among other things, that the ABC ‘seeks to balance the public interest in respect for privacy with the public interest in disclosure of information and freedom of expression’.

and identifiable public interest in the material being broadcast. The public interest is assessed at the time of the broadcast.

Whether something is in the public interest will depend on all the circumstances, including whether a matter is capable of affecting the community at large so that the audience might be legitimately interested in or concerned about what is going on.

...

Any material that invades a person's privacy in the public interest should directly or indirectly contribute to the public's capacity to assess an issue of importance to the public, and its knowledge and understanding of the overall subject. The information disclosed should be proportionate and relevant to those issues, and not include peripheral facts or be excessively prolonged, detailed or salacious.

Whether an invasion of privacy or intrusion into a person's private life is justified in the public interest will generally depend on the public interest matters raised in the broadcast.

5.314 The approach proposed by the NSWLRC considered freedom of speech in the context of the role of the media:<sup>287</sup>

Freedom of speech is a public interest of fundamental importance, and a free press plays a crucial role in preserving and upholding that public interest. What needs to be recognised, however, is that the concept of public interest goes beyond freedom of speech, as [do] the media's responsibilities. In addition to presenting the public with information, the media also play an important role in helping to ensure the public interest in the protection of personal privacy is upheld by not making unwarranted intrusions into privacy in the name of freedom of speech.

5.315 The NSWLRC explained that including the media within their proposed surveillance device scheme was not 'an incursion on freedom of speech', because restrictions on covert information gathering are not necessarily limitations on the freedom of the press or of free speech. It observed that those freedoms are not absolute and that the proposed scheme will ensure that, in upholding those freedoms, the media also respect other relevant public interests.<sup>288</sup>

5.316 However, the NSWLRC did recognise that the issuing authority for its proposed scheme needed to consider all relevant factors, and stated that a relevant factor should be 'the role played by the media in upholding the public interest'. This role includes presenting the public with relevant information, but also 'helping to

<sup>287</sup> NSWLRC Interim Report No 98 (2001) [6.16]. See also [5.293]–[5.294] above.

The terms 'freedom of expression' and 'freedom of speech' are often used to refer to the free speech rights of both individuals and the media: Prof Onora O'Neill, FBA, FRS, FMedSci, Witness Statement for Leveson Inquiry, 14 June 2012, [2]. However, the public interest in individual freedom of expression is distinct from the public interest in press freedom: Leveson Inquiry Report, above n 281, vol 1, 71.

<sup>288</sup> NSWLRC Interim Report No 98 (2001) [6.17]. The NSWLRC also observed that the concept of those freedoms not being absolute is reflected in other legislation applicable to the media, such as defamation.

ensure the public interest in the protection of personal privacy is upheld by not making unwarranted intrusions into privacy in the name of freedom of speech'.<sup>289</sup>

5.317 As explained previously, the ALRC suggested a specific defence of 'responsible journalism', which incorporates the concept of the public interest.<sup>290</sup>

5.318 In other jurisdictions, the use prohibitions in surveillance devices legislation do not include provisions specific to the media. In Western Australia, provisions about the use of a surveillance device in the public interest were intended to ensure that the legislation would have only 'minimal impact' on the media on the 'rare occasions' where covert surveillance was carried out in the public interest.<sup>291</sup> Additionally, this approach 'maintains the privacy rights of the individual by allowing surveillance only when there is a strong public interest in doing so' and, except in an emergency, only with consent.<sup>292</sup>

### ***The Commission's view***

5.319 The draft Bill provides that it is not an offence for a person to use, install or maintain a surveillance device where the use of the device is 'reasonably necessary in the public interest'. It is desirable that media organisations and journalists are subject to the same regulation as others. The Commission is of the view that it is not necessary to make specific provisions about the use of surveillance devices by media organisations and journalists.

5.320 The Commission acknowledges the importance of the public interest in a free press, and the media's role in disseminating information. However, other public and private interests, including the protection of personal privacy, also arise in particular circumstances. In some instances, the balancing of relevant interests will result in those other interests taking priority. This is similar to the balancing exercise required under other rights-based legislation, such as the *Human Rights Act 2019*.<sup>293</sup>

5.321 The requirement for media organisations and journalists to comply with the draft Bill is a reasonable and balanced outcome. The media should, in some circumstances, be permitted to use a surveillance device without consent because it is in the public interest for the media to gather and publish the information they reasonably expect to obtain at the time of using the device. If use that is reasonably necessary in the public interest is an exception to the prohibition against the use of

---

289 NSWLRC Report No 108 (2005) [5.39], [5.47], Rec 3.

290 See [5.296]–[5.297] above.

291 Specifically, the use of a listening device or an optical surveillance device in the public interest is generally permitted with a party's consent, or without consent in an emergency: *Surveillance Devices Act 1998* (WA) ss 26–29.

292 Western Australia, Parliamentary Debates, Legislative Council, 21 October 1998, 2406 (NF Moore, Leader of the House). The same intention to have 'minimal impact' applied in the case of private investigators and the public. It was also observed that 'in most circumstances the work of the media and inquiry agents [or private investigators] involves the surveillance of an activity that will not fall within the definition of private activity'.

293 See *Human Rights Act 2019* (Qld) s 13. See also NSWLRC Interim Report No 98 (2001) [6.17], in which the NSWLRC observed that freedom of speech is not absolute and must sit with other public interests, which in some circumstances should take precedence. This is recognised in law by including media activity within the scope of defamation, contempt and trespass laws.

a surveillance device, media organisations and journalists do not need or have a principled basis for any greater protection.

5.322 It is not necessary to include the role of the media in upholding the public interest as an additional matter for consideration. The list of matters recommended by the Commission is sufficient to deal with the particular roles and interests of media organisations and journalists in the use of surveillance devices.

## Safety and wellbeing

5.323 In some jurisdictions, exceptions permit the use of a listening device or an optical surveillance device in circumstances that are related, generally, to safety and wellbeing.

5.324 In Tasmania, a person may use a listening device to obtain evidence or information connected with an imminent threat of serious violence to a person 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.<sup>294</sup> This exception was ‘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’.<sup>295</sup>

5.325 In Western Australia, a person who has a child or protected person under their care, supervision or authority may use a listening device or an optical surveillance device on their behalf in particular circumstances.<sup>296</sup> Some jurisdictions permit the use of a tracking device to monitor the location of a patient in particular prescribed circumstances, such as where a patient may leave without regard for their health or safety, or to locate a vulnerable patient that is missing or lost.<sup>297</sup>

5.326 The Commission considers that it is appropriate for the draft Bill to include an exception similar to the Tasmanian provision. This approach makes it clear that a person can use a surveillance device to obtain evidence or information in appropriate

<sup>294</sup> *Listening Devices Act 1991* (Tas) s 5(2)(c). 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: ss 5(4)–(7), 6–8.

<sup>295</sup> Tasmania, *Parliamentary Debates*, Legislative Assembly (1 May 1991) 934–5 (PJ Patmore, Minister for Justice).

<sup>296</sup> *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3). See further [5.289] above.

<sup>297</sup> *Surveillance Devices Act* (NT) s 13(2)(d); *Surveillance Devices Regulations* (NT) reg 3(1); *Surveillance Devices Act 1998* (WA) s 7(2)(d); *Surveillance Devices Regulations 1999* (WA) reg 6(1).

The NZLC supported the use of a tracking device where it is no more extensive than reasonably necessary to protect a person’s health, safety or wellbeing, or to protect public health and safety. It explained, by way of example, that this would enable the use of a device to monitor people with dementia so they do not wander and get lost, to allow parents to monitor the location of their children when away from home, and to enable hospitals to track the movements of patients within the hospital: NZLC Report No 113 (2010) [3.54].

The VLRC made a similar recommendation in relation to people with dementia or similar conditions but suggested that, at least in part, this should be achieved by expanding the regime in the *Guardianship and Administration Act 1986* (Vic): VLRC Report No 18 (2010) [6.48] ff.

circumstances, but places a limit on the use of a surveillance device by including the requirement of immediacy.

5.327 The exception should provide that a person is permitted to use, install or maintain a surveillance device to obtain evidence of, or information about, a serious threat to the life, health, safety or wellbeing of an individual, or a serious threat of substantial damage to property. This is consistent with the approach under the *Information Privacy Act 2009*.<sup>298</sup> The term ‘serious threat’ sets an appropriate standard for the application of this exception, and the use of this approach is consistent with other relevant legislation.

5.328 It is not necessary for this exception to refer to an ‘imminent threat’. The exception necessarily requires that a threat be in existence at the time that a surveillance device is used, and requires a belief that it is necessary to use the device immediately. This is a sufficient limit to the application of the exception.

5.329 The exception should include a requirement that the person ‘believes, on reasonable grounds, it is necessary for the device to be used immediately to obtain the evidence or information’. This protects privacy in circumstances where immediate use is not necessary, and requires people to use other appropriate means in those instances (for example, reporting their concerns to the police).

5.330 Accordingly, the draft Bill provides that the use, installation or maintenance of a surveillance device by a person to obtain evidence of, or information about, a serious threat to the life, health, safety or wellbeing of an individual, or of substantial damage to property, is not an offence if the person believes, on reasonable grounds, that it is necessary for the device to be used immediately to obtain the evidence or information.

5.331 Finally, there are specific Acts, such as the *Mental Health Act 2016*, *Disability Services Act 2006* or the *Guardianship and Administration Act 2000*, which establish legislative schemes to provide for the care and wellbeing of a particular cohort of vulnerable people. As a matter of policy, it is appropriate that specific regulation of the use of a surveillance device in connection with a vulnerable person be dealt with under the relevant Act.

## Location and retrieval of a lost or stolen vehicle or other thing

5.332 In New South Wales and South Australia, it is not an offence for a person to use a listening device, an optical surveillance device or (in South Australia) a

<sup>298</sup>

The *Information Privacy Act 2009* prevents the use or disclosure of an individual’s personal information unless ‘the agency is satisfied on reasonable grounds [that it] is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare’: *Information Privacy Act 2009* (Qld) sch 3, IPPs 10(1)(b), 11(1)(c).

The Commission considered adopting similar wording to s 43(2)(e)(iii) of the *Invasion of Privacy Act 1971* (Qld), which provides an exception in relation to officers of government entities where there are ‘reasonable grounds to believe there may be a risk to the life, health or safety’ of an officer. On balance, the Commission has prioritised consistency with the wording in the *Information Privacy Act 2009* (Qld) sch 3, IPPs 10(1)(b), 11(1)(c).

tracking device, if it is used solely for the purposes of locating and retrieving that device.<sup>299</sup>

5.333 In Western Australia, it is not an offence for a person to use a tracking device in relation to an object that:<sup>300</sup>

- (a) was in the person's possession or under the person's control when the device was attached or installed; and
- (b) is no longer in the person's possession or under the person's control; and
- (c) the person reasonably believes to have been stolen.

5.334 A broad exception, such as in New South Wales or South Australia, permits a person to locate and retrieve a surveillance device in any circumstances. Although it is required that the use is 'solely for the purposes of' location and retrieval of the device, this still enables the location and retrieval of a device that is lawfully in another person's possession (for example, a phone that has been borrowed with consent) and this might result in incidentally obtaining information about the other person and their whereabouts.

5.335 It is more appropriate for an exception of this kind to have a narrower application, similar to the provision in Western Australia, but to apply in circumstances where a vehicle or other thing is lost or stolen.

5.336 Accordingly, the draft Bill provides that it is not an offence for a person to use a surveillance device to locate a vehicle or other thing if the person:

- (a) is not in possession or control of the vehicle or thing; and
- (b) believes, on reasonable grounds, that the vehicle or thing is lost or stolen; and
- (c) is an owner of the vehicle or thing or, before the vehicle or thing was lost or stolen, was in lawful control of it.

5.337 This exception could apply to the use of a surveillance device to locate the device itself, or to locate a vehicle or some other thing. For example, a person who has attached a tracking device to their bicycle could, if it is stolen, use that tracking device to find its location.

5.338 This exception allows a person to use a surveillance device for the purpose of locating a vehicle or other thing in circumstances where a person would be entitled to its return, but protects privacy by limiting the exception to those circumstances. It does not allow a person to use a surveillance device to locate or retrieve a vehicle or

<sup>299</sup> *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 in relation to listening devices and optical surveillance devices and also includes 'enhancement equipment' related to those devices. 'Enhancement equipment' is defined as equipment capable of enhancing a signal, image or other information obtained by the use of a surveillance device: s 4(1).

<sup>300</sup> *Surveillance Devices Act 1998* (WA) s 7(2)(d); *Surveillance Devices Regulations 1999* (WA) reg 6(2). This exception is included as a prescribed circumstance: see generally [5.347] ff below.



other thing if the person was not, prior to it being lost or stolen, an owner or person in lawful control of it.

### Authorised under another Act of the State or an Act of the Commonwealth

5.339 Surveillance devices legislation in other jurisdictions includes exceptions for the use of a device that is authorised by another law. Generally, the prohibitions do not apply to the use, installation, maintenance or attachment of a surveillance device that is in accordance with or authorised under the *Telecommunications (Interception and Access) Act 1979* or any other law of the Commonwealth, surveillance devices legislation, or any other Act or a corresponding law.<sup>301</sup>

5.340 There are also exceptions for use of a surveillance device by law enforcement officers, for matters of law enforcement or for other government use (for example, use by fire and emergency services).<sup>302</sup>

5.341 Under the *Invasion of Privacy Act 1971*, the prohibition on the use of listening devices does not apply 'to or in relation to the use of a listening device by a police officer or another person under a provision of an Act authorising the use of a listening device'.<sup>303</sup>

5.342 The draft Bill retains a similar exception in relation to the use prohibitions. It provides that the use, installation or maintenance of a surveillance device without consent is not an offence if it is authorised under another Act of the State or an Act of the Commonwealth. This exception ensures that use of a surveillance device that is expressly authorised by another Act is not affected.<sup>304</sup> Such authorising Acts include:

- the PPRA, which regulates the use of a surveillance device by police officers in certain circumstances,<sup>305</sup> and makes lawful the use of a body-worn camera

<sup>301</sup> *Listening Devices Act 1992* (ACT) ss 3B, 3C, 4(2)(a); *Surveillance Devices Act 2007* (NSW) ss 7(2)(b), 8(2)(b), 9(2)(b), 10(2)(b); *Surveillance Devices Act* (NT) ss 11(2)(a)(ii), 12(2)(b), 13(2)(b), 14(2)(b), pt 6; *Surveillance Devices Act 2016* (SA) ss 4(2)(b)(i)–(ii), 5(4)(a)(i)–(ii), (c), (d), 7(2)(a)(i)–(ii), 8(2)(a); *Listening Devices Act 1991* (Tas) s 5(2)(b); *Surveillance Devices Act 1999* (Vic) ss 6(2)(b), 7(2)(b), 8(2)(b), 9(2)(b); *Surveillance Devices Act 1998* (WA) ss 5(2)(c), 6(2)(c), 7(2)(e).

Some jurisdictions, such as the Australian Capital Territory and Victoria, provide more specifically that the Act does not apply to the use of a device in relation to particular listed Acts, or to the use of a device under a law of the Commonwealth.

<sup>302</sup> *Surveillance Devices Act 2007* (NSW) ss 7(2)(a), (d), (f), (4), 8(2)(a), (d)–(f), 9(2)(a), 10(2)(a), pts 3–6; *Surveillance Devices Act* (NT) ss 11(2)(a)(i), (b), (ba), 12(2)(a), (c)–(da), 13(2)(a), (c), 14(2)(a), 14A, pts 4–5, 7–8; *Surveillance Devices Act 2016* (SA) ss 4(2)(b)(iii), (d), (e), 5(4)(a)(iii), (c), (d), 7(2)(a)(iii), pts 3–4; *Listening Devices Act 1991* (Tas) s 5(2)(a), (ba)–(bb), (e), pt 4; *Surveillance Devices Act 1999* (Vic) ss 6(2)(a), (c)–(e), 7(2)(a), (c)–(e), 8(2)(a)–(ad), 9(2)(a), pts 4–5; *Surveillance Devices Act 1998* (WA) ss 5(2)(a)–(b), (3)(a)–(b), 6(2)(a)–(b), (3)(b)(i)–(ii), 7(2)(a)–(c), pt 4.

<sup>303</sup> *Invasion of Privacy Act 1971* (Qld) s 43(2)(d). The Act also includes exceptions related to people employed in connection with the Commonwealth and to government network radios. These are addressed separately below: see *Invasion of Privacy Act 1971* (Qld) s 43(2)(c), (e); [11.15] ff below.

<sup>304</sup> The draft Bill would not affect the operation or application of other relevant laws, for example, the Criminal Code (Qld).

<sup>305</sup> *Police Powers and Responsibilities Act 2000* (Qld) ch 13. Under the PPRA, a 'surveillance device' includes a listening device, an optical surveillance device, a tracking device and a data surveillance device, and a device that is a combination of any two or more of those devices: s 322 (definition of 'surveillance device').

by police officers;<sup>306</sup>

- the *Commissions of Inquiry Act 1950*, which regulates the use of a listening device by commissions of inquiry in certain circumstances;<sup>307</sup>
- the *Crime and Corruption Act 2001*, which regulates the use of a surveillance device by commission officers in certain circumstances;<sup>308</sup>
- the *Fisheries Act 1994*, which makes lawful the use of a body-worn camera by inspectors,<sup>309</sup> and the use of vessel tracking equipment by relevant boats;<sup>310</sup>
- the *Public Safety Preservation Act 1986*, which regulates the use of a surveillance device in an emergency;<sup>311</sup>
- the *Youth Justice Act 1992*, which makes lawful the recording of images or sounds in a detention centre, and the authorised use of a body-worn camera by detention centre employees;<sup>312</sup>
- the *Corrective Services Act 2006*, which provides that some prisoner communications or personal visits may be monitored or recorded, and that an offender may be required to wear a device, or permit installation of a device or equipment at their residence, to enable the monitoring of their location;<sup>313</sup>

<sup>306</sup> *Police Powers and Responsibilities Act 2000* (Qld) s 609A. Section 609A(4) explicitly states that, '[t]o remove any doubt, it is declared that subsection (1) is a provision authorising the use by a police officer of a listening device, for the purposes of the *Invasion of Privacy Act 1971* (Qld), section 43(2)(d)'.

<sup>307</sup> *Commissions of Inquiry Act 1950* (Qld) ss 3 (definition of 'listening device'), 19C.

<sup>308</sup> *Crime and Corruption Act 2001* (Qld) ch 3 pt 6. Schedule 2 of that Act defines a 'surveillance device' to mean:

- (a) for a crime investigation—
  - (i) a listening device; and
  - (ii) a visual surveillance device; and
  - (iii) a tracking device; and
  - (iv) a device containing any combination of the devices mentioned in subparagraphs (i), (ii) and (iii); and
  - (v) a data surveillance device; and
- (b) for a corruption investigation—a listening device.

<sup>309</sup> *Fisheries Act 1994* (Qld) s 181A(1). Section 181A(4) explicitly states that, '[t]o remove any doubt, it is declared that subsection (1) is a provision authorising the use by an inspector of a listening device, for the purposes of the *Invasion of Privacy Act 1971* (Qld) s 43(2)(d)'.

<sup>310</sup> *Fisheries Act 1994* (Qld) s 80.

<sup>311</sup> *Public Safety Preservation Act 1986* (Qld) s 43E. The schedule to that Act defines 'surveillance device' by reference to the definition of 'surveillance device' in the PPRa. See also n 305 above.

<sup>312</sup> *Youth Justice Act 1992* (Qld) s 263A(1), (2), (6). Section 263A(7) explicitly states that '[t]o remove any doubt, it is declared that subsections (1), (2) and (6) are provisions authorising the use by the chief executive, or a detention centre employee, of a listening device for the *Invasion of Privacy Act 1971* (Qld) s 43(2)(d)'.

<sup>313</sup> *Corrective Services Act 2006* (Qld) ss 52, 158, 200A, 267. See also, as to monitoring an offender's locations, the *Dangerous Prisoners (Sexual Offenders) Act 2003* (Qld) s 16A.

- the *Bail Act 1980*, which provides that a condition of a person's bail may be that a person wear a tracking device whilst they are released on bail;<sup>314</sup>
- the *Transport Operations (Passenger Transport) Regulation 2018*, which includes requirements for security cameras systems in a booked hire vehicle, limousine or taxi;<sup>315</sup> and
- various Acts which provide that an inspector or authorised officer may (among other things) enter a place, and record, photograph or film any part of the place or anything at the place.<sup>316</sup>

5.343 There might be some instances where the use of a device is not expressly authorised by another Act, for example, where an Act includes a requirement to monitor something without specifying how that monitoring should be carried out. A surveillance device might be used to satisfy that requirement.

5.344 Acts that might authorise or require surveillance or monitoring activities, without expressly authorising the use of a surveillance device, include:

- the *Biosecurity Act 2014*, which provides for the authorisation of 'surveillance programs' directed at monitoring compliance, or identifying and monitoring biosecurity matter;<sup>317</sup>
- the *Food Production (Safety) Regulation 2014*, which provides that Safe Food Production Queensland may monitor compliance with food safety schemes and defines 'monitor' to mean carrying out activities, including, for example, oversight or surveillance of a business;<sup>318</sup>
- the *Marine Parks Act 2004*, *Nature Conservation Act 1992* and *Wet Tropics World Heritage Protection and Management Act 1993*, which variously

<sup>314</sup> *Bail Act 1980* (Qld) s 11(9B). For the purposes of that Act, a 'tracking device' means 'an electronic device capable of being worn, and not removed, by a person for the purpose of the Queensland police service, or the chief executive of the department in which the *Corrective Services Act 2006* (Qld) is administered, finding or monitoring the geographical location of the person': s 11(10).

<sup>315</sup> *Transport Operations (Passenger Transport) Regulation 2018* (Qld) pt 9.

<sup>316</sup> See, eg, *Planning Act 2016* (Qld) s 198; *Fisheries Act 1994* (Qld) s 150; *Fair Trading Inspectors Act 2014* (Qld) s 38; *Liquor Act 1992* (Qld) s 178; *Gaming Machine Act 1991* (Qld) s 329; *Keno Act 1996* (Qld) s 180; *Lotteries Act 1997* (Qld) s 166; *Charitable and Non-Profit Gaming Act 1999* (Qld) s 125; *Wine Industry Act 1994* (Qld) s 49; *Wagering Act 1998* (Qld) s 246; *Taxation Administration Act 2001* (Qld) s 96; *First Home Owner Grant Act 2000* (Qld) s 39; *Food Act 2006* (Qld) s 182; *Tobacco and Other Smoking Products Act 1998* (Qld) s 37; *Public Health Act 2005* (Qld) s 399; *Pest Management Act 2001* (Qld) s 69; *Water Fluoridation Act 2008* (Qld) s 40; *Radiation Safety Act 1999* (Qld) s 117; *Public Health (Infection Control for Personal Appearance Services) Act 2003* (Qld) s 86; *Private Health Facilities Act 1999* (Qld) s 99; *Pharmacy Business Ownership Act 2001* (Qld) s 156; *Health Act 1937* (Qld) s 151; *Racing Integrity Act 2016* (Qld) s 175; *Food Production (Safety) Act 2000* (Qld) s 95; *Nature Conservation Act 1992* (Qld) s 147; *Environmental Protection Act 1994* (Qld) s 460; *Waste Reduction and Recycling Act 2011* (Qld) s 211; *Coastal Protection and Management Act 1995* (Qld) s 134; *Queensland Heritage Act 1992* (Qld) s 139; *Marine Parks Act 2004* (Qld) s 66; *Recreation Areas Management Act 2006* (Qld) s 157; *Wet Tropics World Heritage Protection and Management Act 1993* (Qld) s 70.

Some Acts also provide that a particular person can record information that is given by a person: see, eg, *Taxation Administration Act 2001* (Qld) s 89; *State Penalties Enforcement Act 1999* (Qld) s 134E.

<sup>317</sup> *Biosecurity Act 2014* (Qld) ch 9. However, that Act also provides that 'aerial control measures', which can include activities done from the air by an airborne machine, might be part of a surveillance program. This provision could capture the use of a drone: s 294.

<sup>318</sup> *Food Production (Safety) Regulation 2014* (Qld) s 45, sch 13 (definition of 'monitor').

contain requirements to manage an area (or similar) in a way that allows study and monitoring of that area, to assess or monitor areas as required under the Acts, and to monitor and enforce compliance with the Acts;<sup>319</sup>

- generally, some entities, including government bodies and private business, might use a surveillance device for general purposes such as administering and enforcing legislation, operational monitoring or recording, protecting people and assets, detecting and obtaining evidence of offences committed on their property, and conducting inspections of their own assets or as part of their business (for example, using a drone to inspect a location where access is difficult or dangerous).

5.345 The Commission does not consider that the draft Bill should include an exception for the use of a surveillance device in those circumstances, as it would be very broad. In appropriate circumstances, one of the other exceptions to the use prohibitions, particularly the exception for use that is reasonably necessary in the public interest may apply.<sup>320</sup>

5.346 If specific provisions are required to regulate additional uses of a surveillance device, they could be included as a prescribed circumstance or, alternatively, specifically authorised.

### Prescribed circumstances

5.347 In several jurisdictions, 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,<sup>321</sup> but in the Northern Territory and Western Australia this is limited to a tracking device.<sup>322</sup>

5.348 In relation to a tracking device, prescribed circumstances include:<sup>323</sup>

- to search for a person or thing during a search and rescue operation;

<sup>319</sup> *Marine Parks Act 2004* (Qld) ss 5(2)(i), 66(3), 128; *Nature Conservation Act 1992* (Qld) ss 16(1)(b), 21B(2)(a), 70JB, 73(b), 145; *Wet Tropics World Heritage Protection and Management Act 1993* (Qld) ss 10(1)(l), 68, 71, sch 1. Other Acts also contain various requirement to monitor land: see, eg, *Environmental Protection Act 1994* (Qld) ss 264, 331, 363N, 389. More generally, surveillance devices might be used to monitor areas or to monitor compliance with an Act, without reference to any particular legislative monitoring requirement.

In respect of monitoring compliance with an Act, there may be overlap with the provisions of inspectors or authorised officers, discussed at [5.242] and n 316 above.

<sup>320</sup> In some cases, the types of use that might be required are unlikely to come within the use prohibitions, because they would not relate to private conversations or activities, or to information about an individual's location or information that is input into, output from or stored in a computer.

<sup>321</sup> *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.

<sup>322</sup> *Surveillance Devices Act* (NT) s 13(2)(d); *Surveillance Devices Act 1998* (WA) s 7(2)(d).

<sup>323</sup> *Surveillance Devices Regulations* (NT) reg 3(1); *Surveillance Devices Regulations 2017* (SA) reg 11; *Surveillance Devices Regulations 1999* (WA) reg 6(1), (2). Most circumstances that relate to use in connection with a person (for example, a patient or a person in the criminal justice system) specify that the use is to be by or in accordance with the directions of a person in charge, manager, public authority, or other similar person.

- to monitor the location of a hospital or nursing home patient if the patient is legally obliged to stay but likely to attempt to leave, ill or incapacitated and likely to leave without due regard to their health or safety, or likely to be unlawfully taken from the hospital or nursing home; or to locate a vulnerable patient if the patient becomes lost or goes missing;
- to monitor the activities and/or location of an accused person, offender or prisoner, to locate a prisoner if they escape from legal custody, or for the purposes of specific legislation that relates to bail, sexual offenders or sentencing;
- to monitor the location of an animal or thing the subject of a research project, or an object if its geographical location is relevant to research being carried out by a researcher;
- to measure transport system performance, or monitor traffic on a highway or main road; or
- to track an object that is believed to have been stolen.

5.349 The draft Bill enables additional circumstances in which the use, installation or maintenance of a surveillance device is not an offence to be prescribed by regulation. The ability to prescribe additional circumstances in which the use of a surveillance device is not an offence is prudent and gives the draft Bill some flexibility, while the requirement for this to be prescribed through regulation provides for an appropriate degree of oversight.

5.350 If the use of a surveillance device is permitted or authorised under other legislation then, to remove any doubt, the use of a device for the purpose of that legislation could be listed as a prescribed circumstance.

## Security providers and insurance adjusters

5.351 The *Security Providers Act 1993* provides a scheme for the licensing and regulation of security providers, including private investigators, crowd controllers and security officers.<sup>324</sup>

5.352 A private investigator is a person who, for a reward:<sup>325</sup>

- obtains and gives private information about another person, without the other person's express consent; or

<sup>324</sup> See generally *Security Providers Act 1993* (Qld) ss 4–8A, pt 2. See also: QLRC Consultation Paper No 77 (2018) [3.142]–[3.144].

<sup>325</sup> *Security Providers Act 1993* (Qld) s 6(1). See also: Institute of Mercantile Agents Limited, *Investigators* <[http://www.imal.com.au/index.php?option=com\\_content&view=article&id=34:queensland&catid=25:states-territory-info](http://www.imal.com.au/index.php?option=com_content&view=article&id=34:queensland&catid=25:states-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>>.

- carries out surveillance for obtaining private information<sup>326</sup> about another person, without the other person's express consent; or
- investigates the disappearance of a missing person.

5.353 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.<sup>327</sup>

### **Surveillance devices legislation**

5.354 In South Australia, a licensed investigation agent<sup>328</sup> or a loss adjuster<sup>329</sup> is not prohibited from installing, using or maintaining a listening device or an optical surveillance device if the use is in the course of their functions and is reasonably necessary for the protection of the lawful interests of a person,<sup>330</sup> or if the use is in the public interest.<sup>331</sup>

5.355 Generally, consideration of this topic by the South Australian Legislative Review Committee and the NSWLRC focused primarily on the use of surveillance devices by private investigators to detect insurance fraud, and both recommended schemes that required covert surveillance in those circumstances to be authorised.<sup>332</sup>

<sup>326</sup> 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').

<sup>327</sup> *Security Providers Act 1993* (Qld) s 6(3). In each instance, this also includes an employee of that person.  
An insurance adjuster is bound by the APPs and may be subject to the Insurance Council Code of Practice. Recently, the Insurance Council of Australia recommended that this Code should 'include mandatory standards on the use of investigators and the use of surveillance to ensure that investigations are carried out only when required and in an appropriate manner': Submission 26; Insurance Council of Australia, *General Insurance Code of Practice* (1 July 2014); Insurance Council of Australia, *Final Report: Review of the General Insurance Code of Practice* (June 2018), 51–2, app 5.

<sup>328</sup> 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>>.

<sup>329</sup> 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 at 24 February 2020) 'loss adjuster'.

<sup>330</sup> *Surveillance Devices Act 2016* (SA) ss 4(2)(b)(iv), (v), 5(4)(a)(iv), (v), (5).

<sup>331</sup> *Surveillance Devices Act 2016* (SA) s 6(1)(b), (2)(b).

<sup>332</sup> SA Legislative Review Committee Report (2013) 63–71, 76, Rec 6, which considered the Surveillance Devices Bill 2012 (SA) (not passed); NSWLRC Report No 108 (2005) [5.62]–[5.69], Rec 7. The ACT Review concluded that there should not be particular exceptions for private investigators because in that jurisdiction they are not licenced or subject to a regulatory regime: ACT Review (2016) [2.5](h), [6.34]–[6.38]. See also QLRC Consultation Paper No 77 (2018) [3.146]–[3.147].

### ***The Commission's view***

5.356 The draft Bill does not include specific exceptions relevant to the use, installation or maintenance of surveillance devices by security providers or insurance adjusters. Collectively, the exceptions included in the draft Bill are sufficient to enable the use of surveillance devices by security providers or insurance adjusters in appropriate circumstances.

5.357 Some of the ways that a surveillance device might be used by those people may not fall within the scope of the draft Bill, for example, because the activities monitored are not private activities. Alternatively, the use of a device might fall within the scope of an exception to the use prohibitions, for example, use to detect insurance fraud might be in the public interest.<sup>333</sup>

5.358 Where use of a surveillance device is for the protection of a person's lawful interests, security providers and insurance adjusters could rely on the exception under which a person could be appointed to use a device on another person's behalf for the protection of that other person's lawful interests. It is appropriate that, where a private investigator is acting pursuant to a retainer and their work relates to a private interest, the lawfulness of any use of a surveillance device should stand or fall on the basis of the law applying to the person employing them.

5.359 Additionally, nothing prevents security providers and insurance adjusters from relying on another applicable exception in the draft Bill, which does not require that the person using the device (or using the device on another person's behalf) has any particular role or interest.

### **Not for communication or publication to a person who is not a party**

5.360 In several jurisdictions, a party to a private conversation may use a listening device to record a conversation if it is with the consent of a principal party and not for the purpose of communicating or publishing the conversation, or a report of the conversation, to a person who is not a party to that conversation.<sup>334</sup>

5.361 An exception of this kind is not included in the draft Bill. In the Commission's view, this exception permits the recording of a private conversation without the knowledge of other parties, and therefore effectively permits participant monitoring. As explained previously, the draft Bill does not permit participant monitoring and an exception of this kind would be inconsistent with that approach.

---

<sup>333</sup> For example, the South Australian Legislative Review Committee concluded that detecting insurance fraud represented the 'most significant use of covert surveillance' by licensed agents, and recognised that evidence about whether or not a person has a legitimate insurance claim can be both in the public interest and relevant to protecting a person's lawful interests: SA Legislative Review Committee Report (2013) 76. See also VLRC Report No 18 (2010) [2.81], [2.83]–[2.84].

<sup>334</sup> *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). The VLRC opposed this exception on the basis that it was still possible for the recordings to 'fall into the hands of third parties': VLRC Report No 18 (2010) [6.81].

## Lawful purpose

5.362 In New South Wales, a person may use, maintain or install a tracking device ‘for a lawful purpose’.<sup>335</sup>

5.363 This exception is not included in the draft Bill. The Commission considers that if the use of a device in particular circumstances, or for a particular purpose, is not adequately addressed by the existing exceptions, then that use should be specifically authorised by other legislation or included as a prescribed circumstance in which the use of a surveillance device is not an offence. These approaches are clearer and more targeted, and ensure appropriate oversight.

## RECOMMENDATIONS

### Definitions

**5-1 The draft Bill should define ‘private conversation’ as:**

- (a) Words spoken by an individual are a private conversation if the words are spoken in circumstances that may reasonably be taken to indicate that—**
  - (i) for words not spoken to anyone else—the individual does not want anyone else to listen to the words; or**
  - (ii) for words spoken to another individual, or other individuals—the individual, or at least one of the individuals to whom the words are spoken, does not want the words to be listened to by anyone other than—**
    - (A) the individual speaking the words; and**
    - (B) the individuals to whom the words are spoken; and**
    - (C) any other individual who has the consent of all of the individuals mentioned in subparagraphs (A) and (B).**
- (b) However, a private conversation does not include words spoken by an individual in circumstances in which the individual, and all of the individuals to whom the words are spoken, ought reasonably to expect that someone else may listen to, monitor or record the words.**

***[See Surveillance Devices Bill 2020 cl 11, and [5.162]–[5.172] above.]***

<sup>335</sup>

*Surveillance Devices Act 2007* (NSW) s 9(2)(c). The VLRC expressed the view that this exception is ‘vague and unnecessarily broad’, and suggested that other options, such as exempting particular purposes by regulation, would be preferable: VLRC Report No 18 (2010) [6.42]–[6.44].



**5-2 The draft Bill should define ‘private activity’ as:**

- (a) An activity is a private activity if it is carried out in circumstances that may reasonably be taken to indicate that—**
  - (i) for an activity carried out by one individual—the individual does not want anyone else to observe the activity; or**
  - (ii) for an activity carried out by two or more individuals—at least one of the individuals does not want the activity to be observed by anyone other than—**
    - (A) the individuals carrying out the activity; and**
    - (B) any other individual who has the consent of all of the individuals carrying out the activity.**
- (b) However, a private activity does not include an activity carried out by one or more individuals in circumstances in which all of the individuals carrying out the activity ought reasonably to expect that someone else may observe, monitor or visually record the activity.**

*[See Surveillance Devices Bill 2020 cl 12, and [5.173]–[5.178] above.]*

**5-3 The draft Bill should define ‘party’ as:**

- (a) Each of the following is a party to a private conversation—**
  - (i) an individual who speaks, or is spoken to, during the conversation;**
  - (ii) an individual who listens to the conversation with the consent of all of the individuals mentioned in paragraph (i).**
- (b) Each of the following is a party to a private activity—**
  - (i) an individual carrying out the activity;**
  - (ii) an individual who observes the activity with the consent of all of the individuals mentioned in paragraph (i).**

*[See Surveillance Devices Bill 2020 cl 13, and [5.196]–[5.203] above.]*

**5-4 The draft Bill should explain that, in the legislation, a reference to installing a surveillance device includes doing anything to, or in relation to, a device to enable it to be used as a surveillance device.**

*[See Surveillance Devices Bill 2020 cl 15, and [5.140]–[5.144] above.]*

**5-5** The draft Bill should define ‘maintain’, in relation to a surveillance device, to include:

- (a) adjust, relocate, repair or service the device; and
- (b) replace a faulty device.

*[See Surveillance Devices Bill 2020 sch 1 (definition of ‘maintain’), and [5.137]–[5.139] above.]*

**5-6** The draft Bill should explain that a reference to a person who owns a vehicle, computer or other thing does not include a person (an ‘excluded owner’) who owns the vehicle, computer or other thing if:

- (a) another person has the use or control of the vehicle, computer or other thing under a credit agreement, hiring agreement, hire-purchase agreement, leasing agreement or another similar agreement; and
- (b) under the agreement, the excluded owner is not entitled to immediate possession of the vehicle, computer or other thing.

*[See Surveillance Devices Bill 2020 cl 16, and [5.216]–[5.218] above.]*

#### **Prohibitions on the use, installation or maintenance of surveillance devices**

**5-7** The draft Bill should provide that a person must not use, install or maintain a listening device to listen to, monitor or record a private conversation without the consent of each party to the conversation.

*[See Surveillance Devices Bill 2020 cl 18, [5.148]–[5.151] and [5.207]–[5.211] above.]*

**5-8** The draft Bill should provide that a person must not use, install or maintain an optical surveillance device to observe, monitor or visually record a private activity without the consent of each party to the activity.

*[See Surveillance Devices Bill 2020 cl 19, [5.152] and [5.207]–[5.211] above.]*

**5-9** The draft Bill should provide that a person must not use, install or maintain a tracking device to find, monitor or record the geographical location of:

- (a) an individual without the consent of the individual; or
- (b) a vehicle or other thing without the consent of each person who owns, or is in lawful control of, the vehicle or thing.

*[See Surveillance Devices Bill 2020 cl 20, [5.153] and [5.212]–[5.224] above.]*

- 5-10** The draft Bill should provide that a person must not use, install or maintain a data surveillance device to access, monitor or record information that is input into, output from or stored in a computer without the consent of each person who owns, or is in lawful control of, the computer.

*[See Surveillance Devices Bill 2020 cl 21, [5.154] and [5.225]–[5.234] above.]*

- 5-11** The draft Bill should provide that a person who contravenes a prohibition in Recommendations 5-7 to 5-10 commits an offence, which is punishable by a maximum penalty of 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cll 18, 19, 20, 21, and [5.235]–[5.237] above.]*

**Exceptions to the prohibitions on the use, installation or maintenance of surveillance devices**

- 5-12** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if use of the device is reasonably necessary to protect the lawful interests of:

- (a) the person; or
- (b) if another person has authorised the person to use the surveillance device on the other person's behalf—the other person.

*[See Surveillance Devices Bill 2020 cl 22, and [5.268]–[5.282] above.]*

- 5-13** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if use of the device is reasonably necessary in the public interest.

*[See Surveillance Devices Bill 2020 cl 23(1), and [5.298]–[5.308] above.]*

- 5-14** For the purposes of Recommendation 5-13, in deciding whether the use of a surveillance device is reasonably necessary in the public interest, a court must consider the following matters as they existed when the person used, installed or maintained the device:

- (a) the subject matter of the use of the device;
- (b) the information that the person reasonably expected would be obtained from the use of the device;

- (c) the purpose for which the person intended to use information that the person reasonably expected would be obtained from the use of the device;
- (d) the nature of the public interest that arose in the circumstances;
- (e) whether the public interest could have been served in another reasonable way;
- (f) the extent to which the use, installation or maintenance of the device affected, or was likely to affect, the privacy of an individual;
- (g) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

*[See Surveillance Devices Bill 2020 cl 23(2), and [5.304]–[5.307] above.]*

- 5-15** The draft Bill should provide that a person who uses, installs or maintains a surveillance device to obtain evidence of, or information about, a serious threat does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the person believes, on reasonable grounds, it is necessary for the device to be used immediately to obtain the evidence or information.

*[See Surveillance Devices Bill 2020 cl 24(1), and [5.323]–[5.331] above.]*

- 5-16** For the purposes of Recommendation 5-15, the draft Bill should define the term ‘serious threat’ to mean:

- (a) a serious threat to the life, health, safety or wellbeing of an individual; or
- (b) a serious threat of substantial damage to property.

*[See Surveillance Devices Bill 2020 cl 24(2), and [5.327] above.]*

- 5-17** The draft Bill should provide that a person who uses a surveillance device to locate a vehicle or other thing does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the person:

- (a) is not in possession or control of the vehicle or thing; and
- (b) believes, on reasonable grounds, that the vehicle or thing is lost or stolen; and
- (c) is an owner of the vehicle or thing or, before the vehicle or thing was lost or stolen, was in lawful control of it.

*[See Surveillance Devices Bill 2020 cl 25, and [5.332]–[5.338] above.]*

**5-18** The draft Bill should provide that a person who uses, installs or maintains a surveillance device does not commit an offence against the prohibitions in Recommendations 5-7 to 5-10 if the use, installation or maintenance is:

- (a) authorised under another Act of the State or an Act of the Commonwealth; or
- (b) in circumstances prescribed by regulation.

*[See Surveillance Devices Bill 2020 cl 26, and [5.339]–[5.350] above.]*



## Chapter 6

# Criminal prohibitions on the communication or publication of surveillance information

INTRODUCTION .....	137
SURVEILLANCE DEVICES LEGISLATION .....	138
Queensland .....	138
Other jurisdictions .....	140
SUBMISSIONS.....	143
Communication or publication prohibitions .....	143
Exceptions to the communication or publication prohibitions .....	144
THE COMMISSION'S VIEW .....	148
The approach of the draft Bill .....	148
ELEMENTS OF THE COMMUNICATION OR PUBLICATION PROHIBITIONS .....	149
Intention or knowledge .....	149
Surveillance information that the communication or publication prohibitions apply to.....	149
Consent .....	150
Criminal penalty.....	150
EXCEPTIONS TO THE COMMUNICATION OR PUBLICATION PROHIBITIONS .....	151
Communication or publication in legal proceedings.....	152
Communication or publication to protect that person's lawful interests .....	153
Communication or publication in the public interest.....	156
Communication or publication for safety and well-being .....	161
Communication or publication authorised under another Act or prescribed by regulation .....	162
Communication or publication by security providers and loss adjusters .....	163
Communication or publication to a person with a reasonable interest in the circumstances .....	164
Communication or publication in the performance of a duty.....	164
Communication or publication by a person who obtained knowledge other than by unlawful use of the device .....	166
Communication or publication to a party.....	166
RECOMMENDATIONS .....	167

## INTRODUCTION

6.1 The terms of reference require the Commission to regulate the communication or publication of information derived from surveillance devices.<sup>1</sup>

---

1

See terms of reference, para 2 in Appendix A.

6.2 In the Consultation Paper, the Commission sought submissions about how the communication or publication of information obtained from the lawful or unlawful use of a surveillance device should be dealt with.<sup>2</sup>

## SURVEILLANCE DEVICES LEGISLATION

6.3 Surveillance devices legislation generally prohibits the communication or publication of information obtained from the use of a surveillance device (the ‘communication or publication prohibitions’), subject to exceptions.<sup>3</sup>

6.4 Their purpose is to protect the privacy of an individual from unjustified interference from the communication or publication of such information without consent.

6.5 The communication or publication prohibitions apply variously to information that was obtained lawfully or unlawfully. Generally, ‘unlawfully’ obtained information refers to information obtained in contravention of the use prohibitions, or of the relevant surveillance devices legislation. Information that was obtained ‘lawfully’ refers to information obtained without contravening the use prohibitions, for example, where a person uses a surveillance device with consent or where the particular use of the device falls within an exception to a prohibition.

6.6 The communication or publication of information may be done in various ways including, for example, telling another person about the information, putting the information on social media, or publishing a newspaper article about the information.

## Queensland

6.7 In Queensland, the *Invasion of Privacy Act 1971* contains two communication or publication prohibitions, each with its own exceptions.

6.8 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

<sup>2</sup> QLRC Consultation Paper No 77 (2018) Q-15 to Q-19, Q-21. In particular, the Commission sought submissions on whether the communication or publication of information should:

- if obtained from the unlawful use of a surveillance device—be generally prohibited or prohibited in particular circumstances; and
- if obtained from the lawful use of a surveillance device—be generally permitted or permitted in particular circumstances.

The Commission also sought submissions on whether there should be any special provision in relation to the communication or publication of information obtained through the prohibited or permitted use of a surveillance device by a journalist or media organisation, a private investigator or loss adjuster, or in any other circumstances.

The Commission also sought submissions on whether the communication or publication prohibitions should be punishable as a criminal offence or civil penalty, or both: see [5.28]–[5.30] above.

<sup>3</sup> *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. The prohibitions apply, variously, to information derived from, or that the person knows was obtained as a result of, the use of a surveillance device, or reports or records of information made as a result of the use of a surveillance device: see further [6.7]–[6.22] below.



knowledge as a direct or indirect result of the *unlawful* use of a listening device (that is, in a manner that contravenes section 43(1) of the Act.<sup>4</sup>

6.9 The offence does not apply:<sup>5</sup>

- if the communication or publication is made:
  - to a party to the conversation or with the consent, express or implied, of such a party;<sup>6</sup> or
  - in the course of proceedings for an offence against Part 4 of the Act (which regulates the use, and the communication or publication of information obtained from the use, of a listening device); or
- to prevent a person who has obtained knowledge of a private conversation in a manner that does not contravene section 43(1) of the Act from communicating or publishing that knowledge to another person, even if the person also obtained knowledge of the conversation through the unlawful use of a listening device.

6.10 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, which is *lawful* under the Act, to communicate or publish to another person any record of the conversation made, directly or indirectly, by the use of the listening device or any statement prepared from such a record.<sup>7</sup>

6.11 This offence does not apply where the communication or publication is:<sup>8</sup>

- 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

---

<sup>4</sup> Section 43(1) prohibits the use of a listening device to overhear, record, monitor or listen to a private conversation, except in particular circumstances: see [5.4] above.

<sup>5</sup> *Invasion of Privacy Act 1971* (Qld) s 44(2).

<sup>6</sup> As to the meaning of a 'party' to the conversation, see [2.23], [5.196] above.

<sup>7</sup> Or to communicate or publish a statement prepared from such a record: *Invasion of Privacy Act 1971* (Qld) s 45(1). Participant monitoring is permitted under the *Invasion of Privacy Act 1971* (Qld): see [2.22], [5.245] ff above.

<sup>8</sup> *Invasion of Privacy Act 1971* (Qld) s 45(2).

- for the protection of that party'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
- authorised under the Act or another Act.

## Other jurisdictions

6.12 Like Queensland, the legislation in the Australian Capital Territory and Tasmania contains two communication or publication prohibitions, which generally prohibit the communication or publication of a record or report of a private conversation by:

- any person if it has come to the person's knowledge, or the person knows of the conversation, as a direct or indirect result of the unlawful use of a listening device;<sup>9</sup> and
- a party to a private conversation who lawfully or unlawfully used a listening device to overhear, record, monitor or listen to that conversation.<sup>10</sup>

6.13 In the Northern Territory, Victoria and Western Australia, the legislation contains a single communication or publication prohibition that applies in relation to information obtained from both the lawful and unlawful use of a surveillance device.

6.14 In those jurisdictions, a person must not communicate or publish a record or report of a private conversation or private activity that has come to the person's knowledge, 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 tracking device.<sup>11</sup>

6.15 In contrast, the legislation in New South Wales contains two communication or publication prohibitions, which apply only in relation to information obtained from the unlawful use of a surveillance device

6.16 The first prohibition applies to a record or report of a private conversation or activity that has come to the person's knowledge as a direct or indirect result of use

<sup>9</sup> *Listening Devices Act 1992* (ACT) s 6(1); *Listening Devices Act 1991* (Tas) s 9(1). In those jurisdictions, the offence also applies in relation to the unintentional hearing of a private conversation by means of a listening device. Further, in the Australian Capital Territory, it applies in relation to the lawful use of a listening device with the consent of the parties to the private conversation. In Tasmania, this offence applies if the person 'knowingly' communicates or publishes a record or report of a private conversation.

<sup>10</sup> Those offences apply whether or not the use of the listening device was in contravention of the legislation: *Listening Devices Act 1992* (ACT) s 5(1); *Listening Devices Act 1991* (Tas) s 10(1).

<sup>11</sup> *Surveillance Devices Act* (NT) s 15(1); *Surveillance Devices Act 1999* (Vic) s 11(1); *Surveillance Devices Act 1998* (WA) s 9(1). 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 relevant 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.

of a listening device, an optical surveillance device or a tracking device in contravention of the legislation.<sup>12</sup>

6.17 The second prohibition applies to information regarding the input of information into, or the output of information from, a computer, obtained as a direct or indirect result of the use of a data surveillance device in contravention of the legislation.<sup>13</sup>

6.18 In South Australia, the legislation contains three communication or publication prohibitions that apply to the knowing use, communication or publication of information or material derived from:

- the unlawful use of a surveillance device;<sup>14</sup> and
- the lawful use of a listening device or an optical surveillance device, without consent:<sup>15</sup>
  - to protect that person's lawful interests; or
  - in the public interest.<sup>16</sup>

6.19 In effect, if the use of the device was lawful because it was used with express or implied consent, there is no prohibition on the communication or publication of any information or material derived from that use.<sup>17</sup> Similarly, there is no general prohibition on the communication or publication of information or material

---

<sup>12</sup> *Surveillance Devices Act 2007* (NSW) s 11(1). The scope of the prohibition is limited to the extent that it involves entry into a building or vehicle, or interference with a vehicle or other object, without consent: see [5.182]–[5.184] above.

<sup>13</sup> *Surveillance Devices Act 2007* (NSW) s 14(1). The scope of the prohibition is limited to the extent that the use involves entry onto or into a 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. The legislation in the Northern Territory and Victoria also includes a prohibition on the use of a data surveillance device, which applies to the use of a data surveillance device 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.

<sup>14</sup> *Surveillance Devices Act 2016* (SA) s 12(1). It is an offence for a person to knowingly communicate or publish information or material derived from the use of a listening device, an optical surveillance device, a tracking device or a data surveillance device in contravention of the legislation. The regulation of the use of an optical surveillance device focuses on both the consent of the parties and entry into a building or vehicle, or interference with a vehicle or other object: see [5.182]ff above.

<sup>15</sup> *Surveillance Devices Act 2016* (SA) ss 9(1), 10(1). It is an offence if the communication or publication is done 'knowingly'.

<sup>16</sup> *Surveillance Devices Act 2016* (SA) ss 9(1), 10(1). It is an offence if the communication or publication is done 'knowingly'.

<sup>17</sup> *Surveillance Devices Act 2016* (SA) ss 4(2)(a)(i), 5(1), 7(1), 8(1). In relation to the use of an optical surveillance device, a tracking device or a data surveillance device, express or implied consent is included as an element of the communication or publication use prohibitions. In relation to the use of a listening devices, the offence does not to apply if the device was used by a party to a private conversation to record the private conversation with the express or implied consent of all the principal parties to the conversation. For a discussion of whose consent is required in relation to the use of each device, see [5.204] ff above. For the meaning of principal party, see [5.196]–[5.197] above.

derived from the use of a surveillance device without consent, if the use is captured by an exception to the use prohibitions.<sup>18</sup>

6.20 However, there are particular restrictions that apply to the communication or publication of information obtained from the lawful use of a listening device or an optical surveillance device, without consent, in circumstances where the device was used to protect the lawful interests of that person, or in the public interest. The communication or publication of information obtained in those circumstances is generally prohibited, subject to particular exceptions.<sup>19</sup>

6.21 In each jurisdiction, different exceptions apply to each of the communication or publication prohibitions. They variously include communication or publication:<sup>20</sup>

- with consent;
- in some or all legal proceedings;
- (not more than is reasonably necessary) to protect a person's lawful interests;
- in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;
- (not more than is reasonably necessary) in the public interest;
- (not more than is reasonably necessary) in the performance of a duty;
- to a person with a reasonable interest in the circumstances;
- by a person who obtained knowledge other than by unlawful use of the device; or
- by or to particular authorised persons or as authorised by law.

6.22 The scope and application of the exceptions also varies depending on whether the person was a party to the relevant conversation or activity, the type of surveillance device used and whether the use of the surveillance device was lawful or unlawful.<sup>21</sup>

---

<sup>18</sup> Parliament of South Australia, Report of the Legislative Review Committee into Issues Relating to Surveillance Devices (12 November 2013) 27.

<sup>19</sup> An order of a Supreme Court Judge is generally required prior to communication or publication in the public interest, except for communication or publication to, or by, a media organisation: see further [6.97] below. In relation to communication or publication where a device was used to protect that person's lawful interests, see further [6.87] below.

<sup>20</sup> See further Table 3 in Appendix C.

<sup>21</sup> See further QLRC Consultation Paper No 77 (2018) [3.167] ff.

## SUBMISSIONS

### Communication or publication prohibitions

6.23 Most respondents submitted that the communication or publication of information obtained from the unlawful use of a surveillance device should be generally prohibited, except in particular circumstances.<sup>22</sup>

6.24 The Brisbane City Council observed that the communication or publication of such information should be prohibited because the unlawful use of a surveillance device 'violates the expectation of privacy'. Future Wise similarly noted that the communication or publication of such information 'would undermine the original prohibition' on the unlawful use of a surveillance device. A member of the public also observed that a general prohibition 'will help protect an individual's privacy from further erosion'.<sup>23</sup>

6.25 Additionally, most respondents submitted that the communication or publication of information obtained from the lawful use of a surveillance device should also be prohibited, except in particular circumstances.<sup>24</sup> QAI stated that the communication or publication of lawfully obtained information 'should be subject to stringent safeguards and conditions'. A member of the public noted that 'it should not automatically follow that just because it is legal to 'capture' information, it is also legal to communicate and or publish it'.<sup>25</sup>

6.26 The OIC observed that:<sup>26</sup>

Communication or publication of information obtained through the lawful and unlawful use of a surveillance device is privacy invasive. As outlined in the Consultation Paper, the purpose of [these] legislative provisions is to prevent or limit the damage that could be caused by the communication or publication of information ... without consent.

6.27 An academic gave the example of the use of a camera trap set up in remote bushland to monitor wildlife, or of a drone monitoring vegetation or searching for a lost person. This respondent observed that the use of an optical surveillance device for those purposes is justified and should not constitute an offence. However, its lawful use may inadvertently breach privacy interests, for example, by recording a person who is urinating or who is engaged in sexual activity. For this reason, he submitted that the communication or publication of information recorded by both the lawful and unlawful use of a surveillance device should be generally prohibited.<sup>27</sup>

---

<sup>22</sup> Eg, Submissions 13, 15, 18, 19, 25, 33, 35, 36, 38, 39, 40, 43.

<sup>23</sup> Submission 13.

<sup>24</sup> Eg, Submissions 10, 13, 15, 18, 19, 25, 33, 35, 36, 38, 40, 43.

<sup>25</sup> Submission 13.

<sup>26</sup> This respondent further stated that: 'the purpose of these legislative provisions remains the same irrespective of whether the information was obtained through the lawful or unlawful use of a surveillance device'.

<sup>27</sup> Submission 19.

6.28 The AAUS submitted that legislation should prohibit the communication or publication of ‘a private record without the consent of each party reasonably identifiable from that record’.<sup>28</sup>

### Exceptions to the communication or publication prohibitions

6.29 Most respondents submitted that a general prohibition on communication and publication should be subject to particular exceptions.<sup>29</sup> The OIC noted that:

in certain circumstances, the communication or publication of information obtained through the use of a surveillance device will justify an incursion on an individual’s privacy.

6.30 However, the QLS observed that ‘any proposed exceptions should be carefully considered’ and that it is ‘critical to ensure that no unintended consequences result’. Similarly, a member of the public noted that ‘the inclusion of any exceptions must be strictly limited so as not to encourage or excuse’ the unlawful use of surveillance devices.<sup>30</sup>

6.31 Respondents expressed general support for a number of exceptions to the general prohibition, for example, where the communication or publication is made:

- to a party or with the consent of the parties to the private conversation or activity;<sup>31</sup>
- in the course of legal proceedings;<sup>32</sup>
- to protect that person’s lawful interests;<sup>33</sup>
- in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;<sup>34</sup>
- in the public interest;<sup>35</sup>
- in the performance of a duty;<sup>36</sup>

---

<sup>28</sup> AAUS and Liberty Victoria Paper (2015) [4.4], Rec 5, adopted in Submission 39 from the AAUS. In that paper, the AAUS and Liberty Victoria suggested the adoption of uniform, harmonised surveillance devices legislation. It suggested that ‘private record’ should be defined to mean a record of a private activity (including a communication), and/or the geographical location of a person or an object that has been made as a direct or indirect result of the use of a surveillance device: see further Recs 1, 4 and 6.

<sup>29</sup> Eg, Submissions 10, 13, 15, 19, 25, 35, 36, 38, 39, 43.

<sup>30</sup> Submission 13.

<sup>31</sup> Eg, Submissions 15, 19, 35, 36, 40.

<sup>32</sup> Eg, Submissions 10, 15, 18, 19, 35, 36, 40.

<sup>33</sup> Eg, Submissions 10, 15, 18, 19, 35, 36.

<sup>34</sup> Eg, Submissions 10, 15, 18, 19, 25, 35, 36.

<sup>35</sup> Eg, Submissions 10, 15, 18, 25, 35, 36.

<sup>36</sup> Eg, Submissions 10, 15, 19, 35, 36, 40.

- to a person with a reasonable interest in the circumstances;<sup>37</sup> or
- by a person who obtained knowledge other than by unlawful use of the device.<sup>38</sup>

6.32 However, some respondents submitted that particular exceptions should apply only if the communication is reasonable and proportionate, or if it is ‘not more than is reasonably necessary’.<sup>39</sup>

6.33 In addition, some respondents noted that the communication or publication of information obtained from the use of a surveillance device should be permitted by law enforcement authorities for the investigation of crime.<sup>40</sup>

6.34 The Department of Agriculture and Fisheries also noted that government departments may undertake surveillance in carrying out their functions. Biosecurity Queensland, for example, undertakes surveillance of a population or area to collect data about the presence, incidence, prevalence or geographical extent of a pest or disease. This may include visual surveillance to monitor wildlife for the purposes of feral animal pest management.<sup>41</sup> In order to ensure government departments are not unduly restricted in carrying out their functions, this respondent submitted that: ‘communication, including sharing of information with other relevant agencies, including enforcement agencies, should also be allowed’.

### ***Communication or publication to protect that person’s lawful interests***

6.35 Some respondents submitted that it should not be an offence 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.<sup>42</sup>

6.36 The OIC stated that the approach in South Australia ‘may provide useful guidance in prescribing exceptions to the communication or publication prohibitions’.<sup>43</sup>

---

<sup>37</sup> Eg, Submissions 15, 19, 36, 40.

<sup>38</sup> Eg, Submissions 15, 19, 36.

<sup>39</sup> Eg, Submissions 19, 25. Future Wise observed that communication or publication in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence, or in the public interest, ‘should be undertaken only in a way that is reasonable and proportionate’. An academic noted that the communication or publication of information in the performance of a duty should be ‘not more than reasonably necessary in the performance of a duty of that person’.

<sup>40</sup> Eg, Submissions 15, 19. The terms of reference exclude from the review Queensland’s existing law regulating the use of surveillance devices for State law enforcement purposes.

<sup>41</sup> This respondent submitted that this type of surveillance ‘is usually undertaken in rural and remote areas’ and ‘any capturing of individuals is inadvertent and uncommon’. It noted that biosecurity surveillance is not ordinarily aimed at individuals, except in rare circumstances, such as a significant biosecurity outbreak, ‘where it is important to monitor and limit the human and vehicular assisted spread of pests and diseases’.

<sup>42</sup> Eg, Submissions 19, 36. See also the submissions on the meaning or scope of ‘lawful interests’ at [5.62]–[5.64] above.

<sup>43</sup> The South Australian provision is discussed at [6.87] below.

### ***Communication or publication in the public interest***

6.37 A number of respondents submitted that the legislation should include a broad exception for communication or publication in the public interest.<sup>44</sup>

6.38 A few respondents expressed the view that the legislation should not include a broad public interest exception. Instead, those respondents submitted that there should be specific provisions to cover, for example, the public interest in media and journalists having an exception, or in private investigators and loss adjusters having an exception.<sup>45</sup>

6.39 The QCCL submitted that the communication or publication of information obtained from the *lawful* use of a surveillance device should only be permitted by consent, in the course of legal proceedings, in the performance of a duty and to a person with a reasonable interest in knowing the truth of the matter. It observed that:

The combined exceptions should allow the disclosure of information in all necessary circumstances. In other words, the combined effect of the exceptions is to reflect the public interest.

6.40 This respondent also submitted that information obtained from the *unlawful* use of a surveillance device should generally be communicated or published only with judicial authority or with the informed consent of the subject of the surveillance.

6.41 In contrast, the Insurance Council of Australia submitted that it is not practical to require judicial authority in each case. It observed that:

in some jurisdictions, communication of the results of surveillance requires a court order. We consider that having to wait for a court to decide whether the results of surveillance can be communicated is not practical and increases litigation and demands on court resources. We note that where concerns in communicating the results of surveillance relate to the privacy of other parties, there are pragmatic solutions available (such as the use of pixilation).

### ***Special provision in relation to the media***

6.42 Future Wise observed that communication or publication by investigative journalists may represent a justifiable exception to the communication or publication prohibitions. However, this respondent submitted that investigative journalists should be required to satisfy a public interest test.

6.43 The QCCL and the QLS expressed support for an exception for responsible journalism in the public interest, as was proposed by the ALRC.<sup>46</sup>

6.44 As noted above, the QCCL submitted that judicial authority should ordinarily be required for a communication or publication in the public interest. However, it

---

<sup>44</sup> Eg, Submissions 10, 15, 18, 25, 35, 36. See further [5.65] ff above.

<sup>45</sup> Eg, Submissions 19, 38, 40, 43.

<sup>46</sup> 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': see further ALRC Report No 123 (June 2014) [14.58]–[14.76], Rec 14-5; QLRC Consultation Paper No 77 (2018) [3.197].



submitted that the one exception should be in the case of responsible journalism. It observed that:

the public interest requires a press which is capable of investigating issues and informing the public about them... We would submit that the commission should follow the lead of the [ALRC] and develop a specific exception for responsible journalism.

6.45 The QCCL also noted, however, that:<sup>47</sup>

there is a clear difference between public interest journalism with an underlying quality of journalistic integrity... and scandalous journalism intended to vilify individuals.

6.46 An academic expressed support for a responsible journalism exception as proposed by the ALRC, but submitted that it should be extended to apply to any person.<sup>48</sup>

6.47 The OIC observed that the approach in South Australia 'may provide useful guidance'.<sup>49</sup>

### ***Special provision in relation to private investigators and loss adjusters***

6.48 Future Wise observed that communication or publication by private investigators and insurance loss adjusters are:

circumstances that represent a justifiable exception to communication and publication of prohibited or permitted surveillance. Surveillance lies at the heart of these professions, and might satisfy the balance of benefits as against the harms.

6.49 However, this respondent observed that communication or publication by private investigators and loss adjusters should be made to appropriate parties only to the extent that is necessary and proportionate for the carriage of the relevant matter.

6.50 As previously discussed, the Insurance Council of Australia submitted that the legislation should not impede the ability of insurers and their agents to appropriately conduct legitimate surveillance activities to investigate fraudulent or exaggerated claims.<sup>50</sup>

6.51 The Brisbane City Council submitted that such matters: 'should be dealt with in the context of legislation relevant to these specific industries and their functions and responsibilities'.

---

<sup>47</sup> The QLS made similar observations: see further [5.95] above.

<sup>48</sup> Submission 19. See also [5.68], [5.96] above.

<sup>49</sup> The South Australian provision is discussed at [6.97] below.

<sup>50</sup> See further the discussion of this submission at [5.87] ff above.

## THE COMMISSION'S VIEW

### The approach of the draft Bill

6.52 In the Commission's view, the regulation of the communication or publication of information obtained from the use of a surveillance device requires a criminal response to protect the privacy of individuals from unjustified interference.<sup>51</sup>

6.53 Accordingly, the draft Bill prohibits a person from communicating or publishing surveillance information without consent. As previously explained, 'surveillance information' is defined the draft Bill as 'information obtained, directly or indirectly, using a surveillance device'.<sup>52</sup>

6.54 The communication or publication prohibitions supplement the use prohibitions. They provide an important additional protection, which recognises the breach of privacy caused by the communication or publication of surveillance information about a private conversation, a private activity, the geographical location of an individual, vehicle or thing, or information that is input into, output from, or stored in, a computer.

6.55 The *Invasion of Privacy Act 1971* contains two separate communication or publication prohibitions. The prohibition in section 44(1) applies where a person communicates or publishes information about a private conversation that was obtained from the unlawful use of a listening device (that is, in contravention of the use prohibition in section 43(1)).<sup>53</sup> The prohibition in section 45(1) applies where a party to a private conversation communicates or publishes information about the conversation that was obtained from the lawful use, by that party, of a listening device (that is, in compliance with section 43(2)(a), which permits participant monitoring).<sup>54</sup>

6.56 However, as participant monitoring is not permitted under the draft Bill,<sup>55</sup> it is unnecessary for the communication or publication prohibitions in the draft Bill to distinguish between information obtained from the use of a surveillance device by a person who is a party to a private conversation or private activity and another person.

6.57 Further, in the Commission's view, consent should generally be required prior to the communication or publication of information obtained from the lawful or unlawful use of a surveillance device. Accordingly, the communication or publication prohibitions in the draft Bill do not distinguish between lawfully and unlawfully obtained surveillance information.

---

<sup>51</sup> See [3.23]–[3.24] above.

<sup>52</sup> See [4.52] above.

<sup>53</sup> See [6.8]–[6.9] above.

<sup>54</sup> See [6.10]–[6.11] above.

<sup>55</sup> See [5.247] ff above.

6.58 The communication or publication prohibitions are subject to exceptions where the communication or publication is for a particular purpose that, in the circumstances, justifies the interference with privacy.<sup>56</sup>

6.59 The specific aspects of the Commission's approach, including the elements of the communication or publication prohibitions and their exceptions, are discussed below.

## ELEMENTS OF THE COMMUNICATION OR PUBLICATION PROHIBITIONS

### Intention or knowledge

6.60 The communication or publication prohibitions in the draft Bill apply if the person making the communication or publication knows, or ought reasonably to know, that the information is surveillance information.

### Surveillance information that the communication or publication prohibitions apply to

6.61 The communication or publication prohibitions in the draft Bill apply to surveillance information about:<sup>57</sup>

- a private conversation;
- a private activity;
- the geographical location of an individual, a vehicle or another thing; and
- information that is input into, output from, or stored in a computer.

6.62 This approach links the communication or publication prohibitions to the privacy interest being protected. It is also consistent with the use prohibitions in the draft Bill.

6.63 The draft Bill defines 'information' to include a record in any form and a document. This will ensure that the communication or publication prohibitions will apply to a recording in any form (including an audio, visual, audio visual record or a record in digital form) or a statement prepared from such a record.<sup>58</sup> It will also apply to a report of, or of the substance, meaning or purport of, for example, a private conversation or private activity.<sup>59</sup> This is consistent with the approach taken in

---

<sup>56</sup> See further [6.69] ff below.

<sup>57</sup> As to the meaning of 'private conversation' and 'private activity', see [5.158] ff above.

<sup>58</sup> Pursuant to s 36, sch 1 of the *Acts Interpretation Act 1954* (Qld), a 'document' includes:

- (a) any paper or other material on which there is writing; and
- (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them; and
- (c) any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device).

<sup>59</sup> The Macquarie Dictionary defines 'information' to mean 'knowledge communicated or received concerning some fact or circumstance' or 'knowledge on various subjects, however acquired'.

section 44(1) of the *Invasion of Privacy Act 1971* and surveillance devices legislation in most jurisdictions.<sup>60</sup>

## Consent

6.64 As discussed above, the Commission considers that consent should ordinarily be required prior to the communication or publication of surveillance information. Accordingly, absence of consent is included in the draft Bill as an element of the communication or publication prohibitions.<sup>61</sup>

6.65 Consent to the communication or publication of surveillance information, which may be express or implied, is required from:<sup>62</sup>

- for a *listening device*—each of the parties to the private conversation;
- for an *optical surveillance device*—each of the parties to the private activity;
- for a *tracking device*:
  - for information about the geographical location of an individual whose location is being tracked—that individual;
  - for information about the geographical location of the vehicle or other thing—each person who owns, or is in lawful control of, the vehicle or thing;
- for a *data surveillance device*—each person who owns, or is in lawful control of, the computer.

6.66 This is similar to the approach taken in the use prohibitions in chapter 5 above.<sup>63</sup>

## Criminal penalty

6.67 The maximum penalty for a contravention of the communication or publication prohibitions under the *Invasion of Privacy Act 1971* for an individual is

---

<sup>60</sup> See [6.8]–[6.9] and [6.12] ff above. In the Australian Capital Territory, Tasmania, New South Wales, the Northern Territory, Victoria and Western Australia, the communication or publication prohibitions apply to records or reports of private conversations or activities. The surveillance devices legislation generally defines a 'record' to include an audio, visual or audio visual record or a record in digital form, or a documentary record or statement prepared from such a record. A 'report' is defined to include a report of the substance, meaning or purport of a private conversation or activity.

Cf in South Australia, the communication or publication prohibitions apply to information or material derived from the use of a surveillance device. The words 'information' and 'material' are not defined in the surveillance devices legislation.

<sup>61</sup> Since a lack of consent is included as an element of the communication or publication prohibitions, the draft Bill does not include consent as an exception. By comparison, s 44(2)(a)(i) and 45(2)(a) of the *Invasion of Privacy Act 1971* (Qld) include consent as an exception.

<sup>62</sup> See further the discussion of consent at [4.99] ff above.

<sup>63</sup> See further [5.204] ff above.

imprisonment for two years or 40 penalty units (\$5338).<sup>64</sup> For a corporation, the maximum penalty by default is 200 penalty units (\$26 690).<sup>65</sup>

6.68 Consistently with the approach taken to the use prohibitions in the draft Bill, the Commission is of the view that a contravention of a communication or publication prohibition should be a criminal offence with a maximum penalty of three years imprisonment or 60 penalty units (\$8007). For a corporation, the maximum penalty would be 300 penalty units (\$40 035).<sup>66</sup>

## EXCEPTIONS TO THE COMMUNICATION OR PUBLICATION PROHIBITIONS

6.69 The communication or publication prohibitions in the draft Bill are subject to exceptions under which it is not an offence to communicate or publish surveillance information, without consent, in circumstances where the interference with privacy is justified. This approach protects privacy while taking into account countervailing interests and justified uses of surveillance devices.

6.70 In summary, the draft Bill provides that it is not an offence to communicate or publish surveillance information, without consent, if the communication or publication is:

- in a legal proceeding;
- reasonably necessary to protect the lawful interests of:
  - the person making the communication or publication; or
  - another person who has authorised the person to communicate or publish the information on their behalf;
- reasonably necessary in the public interest;
- reasonably necessary to lessen or prevent a serious threat:
  - to the life, health, safety or wellbeing of an individual; or
  - of substantial damage to property;
- authorised under another Act; or
- in circumstances prescribed by regulation.

---

<sup>64</sup> *Invasion of Privacy Act 1971* (Qld) ss 44(1), 45(1). The prescribed value of a penalty unit is currently \$133.45: *Penalties and Sentences Act 1992* (Qld) ss 5(1)(e)(i), 5A(1); *Penalties and Sentences Regulation 2015* (Qld) s 3. For an overview of the maximum penalties in other Australian jurisdictions see [2.39] above.

<sup>65</sup> The *Invasion of Privacy Act 1971* (Qld) 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 *Penalties and Sentences Act 1992* (Qld) s 181B.

<sup>66</sup> See [5.235]–[5.237] above. As to corporate officer liability, see [7.52] ff below.

6.71 Also, a person does not commit an offence if the use of a surveillance device to obtain the surveillance information the subject of the communication or publication was authorised under another Act.

6.72 The Commission considers that the exceptions contained in the draft Bill provide for the range of circumstances in which the communication or publication of surveillance information without consent is justified.

### Communication or publication in legal proceedings

6.73 The communication or publication prohibitions in surveillance devices legislation apply to communication or publication of information to a court.<sup>67</sup> However, in each jurisdiction, there is an exception permitting communication or publication in the course of some, or all, legal proceedings.<sup>68</sup>

6.74 The scope of this exception differs depending on whether the communication or publication prohibition applies to information obtained from the *lawful* or *unlawful* use of a surveillance device, or both.<sup>69</sup>

6.75 In Queensland, a person who is not a party to a private conversation may communicate or publish information about a private conversation obtained from the *unlawful* use of a listening device in the course of proceedings for an offence against Part 4 of the *Invasion of Privacy Act 1971*.<sup>70</sup>

6.76 However, a person who is a party to a private conversation who used a listening device to overhear, record, monitor or listen to the conversation, which is lawful under the Act, may communicate or publish information about the private conversation in the course of legal proceedings.<sup>71</sup> 'Legal proceedings' are 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.<sup>72</sup>

<sup>67</sup> 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.

<sup>68</sup> *Listening Devices Act 1992* (ACT) ss 5(2)(c), 6(2)(a)(iii); *Surveillance Devices Act 2007* (NSW) ss 11(2)(a)(iv), 14(2)(a)(iv); *Surveillance Devices Act* (NT) s 15(2)(c); *Invasion of Privacy Act 1971* (Qld) ss 44(2)(a)(ii), 45(2)(b); *Surveillance Devices Act 2016* (SA) ss 9(1)(d), 12(2)(d); *Listening Devices Act 1991* (Tas) s 9(2)(a)(iii), s 10(2)(b); *Surveillance Devices Act 1999* (Vic) s 11(2)(c); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(ix).

<sup>69</sup> Surveillance devices legislation in some jurisdictions also includes separate provisions in relation to the inadmissibility of evidence obtained from the unlawful use of a surveillance device. See [7.63] ff below.

<sup>70</sup> *Invasion of Privacy Act 1971* (Qld) s 44(2)(a)(ii). Part 4 of the Act regulates listening devices, and includes the use prohibition and the communication or publication prohibitions.

<sup>71</sup> *Invasion of Privacy Act 1971* (Qld) s 45(2)(b). See further the discussion of 'participant monitoring' at [5.245] ff above.

<sup>72</sup> *Invasion of Privacy Act 1971* (Qld) s 45(3).

6.77 Similar exceptions are included in surveillance devices legislation in the Australian Capital Territory and Tasmania.<sup>73</sup>

6.78 The surveillance devices legislation in the remaining jurisdictions variously permits communication or publication by a person:<sup>74</sup>

- for information obtained from the unlawful use of a surveillance device—in the course of proceedings for an offence against the surveillance devices legislation (New South Wales, South Australia);<sup>75</sup> or
- for information obtained from the lawful and unlawful use of a surveillance device—in the course of legal proceedings (Northern Territory, Victoria, Western Australia).<sup>76</sup>

### **The Commission's view**

6.79 It is not intended that a person be liable for a contravention of the communication or publication prohibitions by communicating or publishing surveillance information to a court or tribunal. The draft Bill therefore provides that a person does not commit an offence against the communication or publication prohibitions where the communication or publication is in a legal proceeding.

6.80 This exception to the communication or publication prohibitions is not intended to make the information admissible if it is not otherwise admissible in court proceedings.<sup>77</sup>

### **Communication or publication to protect that person's lawful interests**

6.81 The *Invasion of Privacy Act 1971* provides that it is not an offence for a party to a private conversation who used a listening device to communicate or publish a

<sup>73</sup> *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). The exception for communication or publication by a party to the private conversation applies to any 'civil or criminal proceedings' in the Australian Capital Territory and to 'legal proceedings' in Tasmania.

<sup>74</sup> *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).

<sup>75</sup> An exception also expressly permits communication or publication for the purpose of investigating or prosecuting an offence against the communication or publication provisions (in NSW) or the communication and publication provisions and pt 2 of the legislation (in South Australia) : *Surveillance Devices Act 2007* (NSW) ss 11(2)(a)(iii), 14(2)(a)(iii); *Surveillance Devices Act 2016* (SA) ss 9(1)(c), 12(2)(c).

In South Australia, there is also a separate offence provision prohibiting the communication or publication of information obtained from the use of a surveillance device to protect that person's lawful interests. In that case, the information can be communicated or published in the course, or for the purposes, of a relevant action or proceeding, or to an officer of an investigating agency for the purpose of investigating or prosecuting such an offence: *Surveillance Devices Act 2016* (SA) s 9(1)(c)–(d). See n 85 below, in relation to the definition of 'relevant action or proceeding'.

<sup>76</sup> The precise wording is: 'in the course of legal or disciplinary proceedings' (Northern Territory, Victoria); 'in the course of any legal proceedings' (Western Australia).

<sup>77</sup> See [7.63] ff below, in relation to the admissibility of evidence obtained from the unlawful use of a surveillance device.

record of the conversation if the communication or publication is 'not more than is reasonably necessary for the protection of the lawful interests of that person'.<sup>78</sup>

6.82 Similarly, in the Australian Capital Territory and Tasmania, it is not an offence for a party to a private conversation to communicate or publish a record of the conversation if the communication or publication is reasonably necessary to protect the lawful interests of the person making it.<sup>79</sup>

6.83 In the Northern Territory, Victoria and Western Australia, the communication or publication prohibitions do not apply to a communication or publication by a person that is not more than is reasonably necessary for the protection of the lawful interests of the person making the communication or publication.<sup>80</sup>

6.84 Additionally, in the Australian Capital Territory and Western Australia, if a listening device or an optical surveillance 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.<sup>81</sup>

6.85 As previously discussed, 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. The communication or publication must also be 'reasonably necessary' to protect the person's lawful interests, which is to be assessed objectively, taking into account the particular circumstances.<sup>82</sup>

6.86 Surveillance devices legislation in New South Wales and South Australia does not contain a broad exception where communication or publication is made to protect the lawful interests of the person making it. As explained above, the general communication or publication prohibitions in those jurisdictions apply where the information was obtained as a direct or indirect result of the use of a surveillance device in contravention of the surveillance device prohibitions in the legislation.

---

78 *Invasion of Privacy Act 1971* (Qld) s 45(2)(c)(iii). There is no lawful interest exception for communication or publication by a person of a record of a private conversation unlawfully listened to under s 44(2): see [6.8]–[6.9] above.

79 *Listening Devices Act 1992* (ACT) s 5(2)(d); *Listening Devices Act 1991* (Tas) s 10(2)(c). In the Australian Capital Territory, the offence does not apply if the communication or publication 'is considered by the party making it, on reasonable grounds, to be necessary for the protection of that party's lawful interests'. This exemption does not apply if the use of the listening device is by or on behalf of the Territory. In Tasmania, the offence does not apply if the communication or publication 'is not more than is reasonably necessary for the protection of the lawful interests of the person making the communication or publication'.

80 *Surveillance Devices Act* (NT) s 15(2)(b)(ii); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(ii); *Surveillance Devices Act 1998* (WA) s 9(2)(vi), (3)(a)(iii).

81 *Listening Devices Act 1992* (ACT) s 6(2)(a)(iv); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(vii). In the Australian Capital Territory, the exemption does not apply if the use of the listening device is by or on behalf of the Territory.

82 See [5.261] ff above in relation to the meaning of 'lawful interests' and 'reasonably necessary'.



6.87 In South Australia, such an exception was considered ‘too broad’ in relation to the use prohibitions.<sup>83</sup> 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:<sup>84</sup>

- (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;<sup>85</sup> 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];<sup>86</sup> or
- (h) otherwise in the course of duty or as required or authorised by law.  
(notes added)

### ***The Commission’s view***

6.88 The draft Bill provides that it is not an offence to communicate or publish surveillance information if the communication or publication is reasonably necessary to protect the lawful interests of the person making it.

6.89 This exception applies to any person who can establish that they have a lawful interest, and that the communication or publication of surveillance information is reasonably necessary for the protection of that lawful interest.

6.90 It also applies if the communication or publication of surveillance information is reasonably necessary to protect the lawful interests of another person who has

<sup>83</sup> 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).

<sup>84</sup> *Surveillance Devices Act 2016* (SA) s 9(1).

<sup>85</sup> A ‘relevant action or proceeding’ is defined to include a prosecution of an offence, an application for bail, and other specified proceedings or hearings: *Surveillance Devices Act 2016* (SA) s 3(1). Examples of a relevant action or proceeding include a prosecution of an offence, an application for bail, a police disciplinary proceeding; and a proceeding relating to alleged misbehaviour, or alleged improper conduct, of a police officer (however described), or an officer or employee, of the State or another jurisdiction.

<sup>86</sup> 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).

authorised the person to communicate or publish the information on the other person's behalf.

6.91 This exception is consistent with, and a corollary to, the lawful interests exception that applies to the use prohibitions.<sup>87</sup>

### Communication or publication in the public interest

6.92 The *Invasion of Privacy Act 1971* provides that it is not an offence for a party to a private conversation who used a listening device to communicate or publish a record of the conversation if the communication or publication is 'not more than is reasonably necessary in the public interest'.<sup>88</sup>

6.93 In the Northern Territory and Victoria, the legislation provides that it is not an offence to communicate or publish a record or report of a private conversation or a private activity that has come to the person's knowledge as a result of the use of a surveillance device if the communication or publication is not more than is 'reasonably necessary in the public interest'.<sup>89</sup> This exception could, in appropriate circumstances, apply in relation to a media organisation, journalist, private investigator or loss adjuster.

6.94 Surveillance devices legislation in other jurisdictions does not contain a broad exception for communication or publication in the public interest.<sup>90</sup>

6.95 In South Australia and Western Australia, an order of a Supreme Court judge is generally required prior to a communication or publication, in circumstances where a relevant surveillance device was used in the public interest.<sup>91</sup> In Western Australia, it was explained that the requirement for judicial oversight in these

<sup>87</sup> See further [5.268]ff above.

<sup>88</sup> *Invasion of Privacy Act 1971* (Qld) s 45(2)(c)(iii). There is no public interest exception for communication or publication by a person of a record of a private conversation unlawfully listened to under s 44(2): see further [6.9] above.

<sup>89</sup> *Surveillance Devices Act* (NT) s 15(2)(b)(i); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(i). However, in the Northern Territory, the communication or publication of private conversations or private activities obtained from the emergency use of a listening device or an optical surveillance device under pt 6 of the *Surveillance Devices Act* (NT) is subject to judicial oversight: see further [6.96] below.

<sup>90</sup> However, in Western Australia, the other exceptions to the prohibition on communication or publication apply 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).

<sup>91</sup> In South Australia, if a listening device or an optical surveillance device was used in the public interest, information derived from that use cannot be communicated or published except in accordance with an order of a Supreme Court judge: *Surveillance Devices Act 2016* (SA) ss 3(1) (definition of 'judge'), 10(1). However, there is special provision in relation to media organisations: see further [6.97] below.

In Western Australia, it is not an offence to communicate or publish private conversations or private activities obtained from the use of a listening device or an optical surveillance device if the communication or publication is made in accordance with pt 5 of the *Surveillance Devices Act 1998* (WA), which regulates the use of those devices in the public interest, including their emergency use. Under pt 5, a judge may make an order allowing communication or publication in the public interest if they are satisfied 'that the publication or communication should be made to protect or further the public interest'. For the purposes of pt 5, 'public interest' is defined to include 'the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens'. See further *Surveillance Devices Act 1998* (WA) ss 9(2)(a)(viii); pt 5.

circumstances 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.<sup>92</sup>

6.96 In the Northern Territory, the communication or publication of private conversations or private activities obtained from the emergency use of a listening device or an optical surveillance device under Part 6 of the Act is also subject to judicial oversight.<sup>93</sup>

### ***Special provision in relation to the media***

6.97 In South Australia, special provision is made permitting communication or publication to, or by, media organisations in the public interest. In that jurisdiction, there is a general requirement to obtain an order of a Supreme Court Judge 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 used in the public interest.<sup>94</sup> This does not apply if the communication or publication is made:<sup>95</sup>

- to a media organisation; or
- by a media organisation and the information or material is in the public interest.

6.98 The exceptions for a media organisation were included following opposition to an earlier Bill that required, as a blanket rule, an order of a judge prior to any

<sup>92</sup> Western Australia, *Parliamentary Debates*, Legislative Council, 21 October 1998, 2406 (NF Moore, Leader of the House).

<sup>93</sup> See further *Surveillance Devices Act* (NT) pt 6, which provides separately for the emergency use of a listening device or an optical surveillance device 'if at the time of use there are reasonable grounds for believing the circumstances are so serious and the matter is of such urgency that the use of the device is in the public interest'. For the purposes of pt 6, 'public interest' is defined to include 'the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens'. If a person uses a listening device or an optical surveillance device under pt 6, they must provide a written report to a Supreme Court judge within two business days of starting to use the device. They cannot communicate or publish records or reports of private conversations or activities obtained from the emergency use of the device under pt 6 without the order of a Supreme Court judge.

<sup>94</sup> *Surveillance Devices Act 2016* (SA) s 10(1). In the Northern Territory and Western Australia, an order of a Supreme Court Judge is also required prior to communication or publication of a record of a private conversation or activity that has come to the person's knowledge from the emergency use of a listening device or an optical surveillance device in the public interest. In those jurisdictions, a person is permitted to use a listening device or an optical surveillance device to listen to, record, or record visually, observe or monitor a private conversation or private activity 'if at the time of use there are reasonable grounds for believing the circumstances are so serious and the matter is of such urgency' that the use of the device is in the public interest: *Surveillance Devices Act* (NT) ss 43, 44, 46; *Surveillance Devices Act 1998* (WA) ss 26–28, 29, 31.

<sup>95</sup> *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 by a person to a media organisation is also permitted where the surveillance device was used to protect the person's lawful interests: s 9(1)(f).

communication or publication of information obtained from the use of a listening device or an optical surveillance device in the public interest.<sup>96</sup>

### **Other approaches**

6.99 The scope of the public interest exception in surveillance devices legislation has been considered in some law reform reviews and inquiries.

6.100 As previously discussed, in relation to the use of a surveillance device, 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’.<sup>97</sup>

6.101 Accordingly, the NSWLRC recommended that the communication or publication of information obtained through covert surveillance in the public interest should generally 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.<sup>98</sup>

6.102 The NSWLRC considered whether covert surveillance by a media organisation should be exempted, but ultimately concluded that it should not, stating:<sup>99</sup>

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 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.

6.103 The ALRC recommended that, instead of a broad public interest defence, surveillance devices legislation should provide a ‘responsible journalism’ defence

---

<sup>96</sup> 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) in debate on the Surveillance Devices Bill 2014 (SA) cl 9(2). See also [6.124]–[6.125] below, as to use by a private investigator or loss adjuster in the public interest.

<sup>97</sup> NSWLRC Report No 98 (2001) [6.24]–[6.25]. See further [5.295] above.

<sup>98</sup> 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’: at [260]. The NSWLRC affirmed these recommendations in NSWLRC Report No 108 (May 2005) [5.37]–[5.49], Recs 3–5. They have not been implemented. As to the authorisation process recommended by the NSWLRC, see [5.293]–[5.294] above.

<sup>99</sup> 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].

‘relating to matters of public concern and importance’.<sup>100</sup> 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 by the use of a device. However, a distinction was drawn in relation to how this defence would apply to these offences:<sup>101</sup>

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.

6.104 In the ACT Review, it was recommended that the legislation should:<sup>102</sup>

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.

### ***The Commission’s view***

6.105 There will be circumstances where the communication or publication of surveillance information is reasonable and justified in the public interest.<sup>103</sup> Accordingly, the draft Bill provides that it is not an offence to communicate or publish surveillance information, without consent, if communication or publication is reasonably necessary in the public interest.

6.106 The requirement for the communication or publication to be ‘reasonably necessary’ will ensure that the scope of the exception is limited to circumstances where the interference with privacy is justified.<sup>104</sup>

6.107 Consistently with the approach taken to the use prohibitions in Chapter 5 above,<sup>105</sup> the draft Bill provides that, for deciding whether a person’s communication or publication of surveillance information is reasonably necessary in the public

---

<sup>100</sup> ALRC Report No 123 (June 2014) [14.58]–[14.76], Rec 14-5. See [5.296]–[5.297] above. The ALRC did not set out the specific elements of such a defence. However, it noted that ‘it may be appropriate for a defence of responsible journalism to apply only where the surveillance was necessary’.

<sup>101</sup> Ibid [14.61]–[14.62].

<sup>102</sup> ACT Review (2016) [2.5](d), [6.21].

<sup>103</sup> As to the meaning of ‘in the public interest’, and some examples of matters that might be in the public interest, see [5.283]–[5.288] above.

<sup>104</sup> See [5.271], [5.299] above.

<sup>105</sup> See [5.304]–[5.307] above.

interest, a court must consider the following matters as they existed when the person communicated or published the information:

- the subject matter of the surveillance information;
- the scope of the communication or publication;
- the nature of the public interest that arose in the circumstances;
- whether the public interest could have been served in another reasonable way;
- the extent to which the communication or publication affected, or is likely to affect, the privacy of an individual; and
- whether, on balance in the circumstances, the public interest justifies the interference with the privacy of an individual.

6.108 Except for one additional matter, the matters are consistent with the matters to be considered in determining whether the use, installation or maintenance of a surveillance device is ‘reasonably necessary in the public interest’ at the time of the use of the device.

6.109 The additional matter is the ‘scope of the communication’. It would include, for example, to whom the information is communicated or published, the medium by which it is communicated or published, the extent of the communication or publication and the character or tone of the communication or publication.<sup>106</sup>

### ***Media organisations and journalists***

6.110 It is not necessary for the draft Bill to include a specific provision for the communication or publication of surveillance information by media organisations or journalists.<sup>107</sup>

6.111 The public interest exception will have the effect that communication or publication of surveillance information to, or by, the media organisations and journalists will not be an offence, provided that it is ‘reasonably necessary’ in the public interest. The public interest in a free press is fundamental to a liberal democracy. However, it is not absolute; it must be balanced with other countervailing public interests, including privacy.<sup>108</sup>

6.112 The Commission also considers that the matters for consideration in the draft Bill, outlined above, are sufficient to deal with the particular roles and interests of media organisations and journalists when communicating or publishing surveillance information.<sup>109</sup> It is not necessary to include any additional matters for

<sup>106</sup> See, eg, *Channel Seven Perth Pty Ltd v S* (2007) 34 WAR 325 [40], [54]–[57]; *Australian Broadcasting Corporation v SAAW Pty Ltd* [2018] WASCA 29 [27]–[28], [76]–[78].

<sup>107</sup> See also the discussion of the matters for consideration in the use prohibitions at [5.319] ff above.

<sup>108</sup> See [5.310] ff above.

<sup>109</sup> See [6.107] ff above.

consideration that relate specifically to the role of the media in upholding the public interest.<sup>110</sup>

### Communication or publication for safety and well-being

6.113 The surveillance devices legislation in New South Wales, Tasmania, and Western Australia provides that it is not an offence if the communication or publication of information obtained from a relevant use of a surveillance device is made:<sup>111</sup>

- 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
- to police in connection with an indictable drug offence or other indictable matter of the requisite seriousness, or if the person believes on reasonable grounds that it is necessary in connection with an imminent threat of serious violence to a person or substantial damage to property (Western Australia).

6.114 In South Australia, it is not an offence if a person communicates or publishes information or material derived from the use of a listening device or optical surveillance device is to protect the person's lawful interests in relation to a situation where a person is being subjected to violence or there is an imminent threat of violence to a person.<sup>112</sup>

### The Commission's view

6.115 The draft Bill provides that it is not an offence to communicate or publish surveillance information, without consent, if it is reasonably necessary to lessen or prevent a serious threat to the life, health, safety or wellbeing of an individual, or of substantial damage to property. This is broadly consistent with the approach taken to the use prohibitions in Chapter 5 above.<sup>113</sup>

<sup>110</sup> This is consistent with the approach taken in relation to the public interest exception for the use prohibitions: see [5.322].

<sup>111</sup> *Surveillance Devices Act 2007* (NSW) ss 49(1)(definition of 'serious narcotic offence'), 11(2)(b), 14(2)(b); *Listening Devices Act 1991* (Tas) s 3(1) (definition of 'serious narcotic offence'), 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.

<sup>112</sup> *Surveillance Devices Act 2016* (SA) s 3(1) (definitions of 'indictable drug offence' and 'external drug offence'), (1)(e).

<sup>113</sup> See [5.323] ff above.

## Communication or publication authorised under another Act or prescribed by regulation

6.116 Surveillance devices legislation includes exceptions for the communication or publication of information obtained from the use of a surveillance device if the communication or publication is authorised under another Act or by law.<sup>114</sup>

6.117 There are also exceptions for communication or publication by or to particular persons, including by a law enforcement officer for particular law enforcement activities and otherwise relating to the performance of the officer's duty.<sup>115</sup>

6.118 The *Invasion of Privacy Act 1971* currently includes specific exceptions for communication or publication of a record or statement of a private conversation by a Commonwealth officer or other person employed in connection with customs or security who used a listening device in circumstances authorised under the Act, to or in relation to the use of a government network radio operated by a call centre operator for a public safety entity in limited emergency circumstances, or by a police officer or another person who used a listening device under a provision of an Act that authorised the use.<sup>116</sup>

### The Commission's view

6.119 There are other State and Commonwealth Acts that regulate the use of surveillance devices and the communication or publication of information obtained from their use.<sup>117</sup>

6.120 In some instances, another Act will expressly authorise the communication or publication of surveillance information.<sup>118</sup> The draft Bill provides that a person does not commit an offence against the communication or publication prohibitions if the communication or publication of surveillance information is authorised under another Act of the State or an Act of the Commonwealth.

<sup>114</sup> Surveillance devices legislation variously provides that a person does not commit an offence if the person's communication or publication is: 'made under an authority granted by or under a law of the Commonwealth' (Australian Capital Territory); 'authorised by a law of the Commonwealth relating to the security of the Commonwealth' (Northern Territory and Victoria); 'required or authorised by law' (South Australia); or 'pursuant to an authority granted by or under the *Telecommunications (Interception) Act 1979* (Cth) or any other law of the Commonwealth' (Tasmania): *Listening Devices Act 1992* (ACT) s 5(2)(f); *Surveillance Devices Act* (NT) ss 15(2)(f), 16(2)(e); *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) s 11(2)(f). In the Northern Territory and Victoria, the surveillance devices legislation also expressly states that the communication or publication prohibitions do not apply in relation to 'protected information', including information obtained from the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation: *Surveillance Devices Act* (NT) ss 15(2)(d), 16(2)(c), 51; *Surveillance Devices Act 1999* (Vic) s 11(2)(ca), 30D.

<sup>115</sup> *Surveillance Devices Act* (NT) ss 15(2)(e)–(ea), 16; *Surveillance Devices Act 1999* (Vic) ss 11(2)(d), (e), 12; *Surveillance Devices Act 1998* (WA) s 9(2)(a)(iii)–(iv).

<sup>116</sup> *Invasion of Privacy Act 1971* (Qld) ss 43(2)(c)–(e), 45(2)(e).

<sup>117</sup> See [5.342] ff above, in relation to other Acts authorising the use of particular surveillance devices.

<sup>118</sup> See, eg, *Police Powers and Responsibilities Act 2000* (Qld) ch 13, pt 5, div 1, which regulates the use, communication and publication of 'protected information', including any information obtained from the use of a surveillance device under a warrant or emergency authorisation.



6.121 In other instances, another Act may expressly authorise the use of a surveillance device, but not the communication or publication of information obtained from that use. The draft Bill provides that a person who communicates or publishes surveillance information does not commit an offence under the communication or publication prohibitions if the use of a surveillance device to obtain that surveillance information was authorised under another Act of the State or an Act of the Commonwealth. This exception continues the approach in section 45(2)(e) of the *Invasion of Privacy Act 1971*.<sup>119</sup>

6.122 However, the person making the communication or publication must comply with any requirements under the Act authorising the use, communication or publication.<sup>120</sup>

6.123 The draft Bill also provides that a person does not commit an offence against the communication or publication prohibitions if the communication or publication of surveillance information is in circumstances prescribed by regulation. This will enable additional circumstances to be prescribed by regulation and is consistent with the approach taken in relation to the use prohibitions.<sup>121</sup>

### **Communication or publication by security providers and loss adjusters**

6.124 In South Australia, a licensed investigation agent or loss adjuster must not knowingly communicate or publish information or material derived from the use of a listening device or optical surveillance device, except to a prescribed person or class of persons, in prescribed circumstances, or as authorised by or under the *Surveillance Devices Act 2016* (SA) or any other Act or law.<sup>122</sup>

6.125 For a licensed investigation agent:<sup>123</sup>

- prescribed persons and classes of persons are: the clients or employers of the licensed investigation agent and the legal representatives of, and medical practitioners providing services, to 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

<sup>119</sup> A number of those Acts also include provisions regulating the disclosure of confidential or personal information: see, eg, *Corrective Services Act 2006* (Qld) s 341; *Fire and Emergency Services Act 1990* (Qld) s 153A; *Fisheries Act 1994* (Qld) s 217B; *Transport Infrastructure Act 1994* (Qld) s 104.

<sup>120</sup> For example, pursuant to s 19C of the *Commissions of Inquiry Act 1950* (Qld), a person can use a listening device under and in accordance with an approval given to overhear, record, monitor or listen to any private conversation to which the person is not a party. However, the person must not communicate or publish the substance or meaning of that private conversation other than to the chairperson who authorised the person to use the device or other person nominated by the chairperson to receive such information.

<sup>121</sup> See [5.347] ff above.

<sup>122</sup> *Surveillance Devices Act 2016* (SA) s 9(2), (3). As to the definitions of 'licensed investigation agents' and 'loss adjusters': see [5.354] above.

<sup>123</sup> *Surveillance Devices Regulations 2017* (SA) s 12.

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.

### ***The Commission's view***

6.126 The Commission is of the view that it is not necessary for the draft Bill to make special provision in relation to private investigators or loss adjusters. The communication or publication of surveillance information by private investigators or loss adjusters is adequately captured by the exceptions included in the draft Bill, including the exception for communication or publication of surveillance information where it is reasonably necessary in the public interest or to protect a person's lawful interests.

### **Communication or publication to a person with a reasonable interest in the circumstances**

6.127 Section 45(2)(d) of the *Invasion of Privacy Act 1971* provides that a party to a private conversation who used a listening device to overhear, record, monitor or listen to that conversation does not commit an offence by communicating or publishing a record of the conversation, or a statement prepared from the record, to a person who has, or who 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'.<sup>124</sup>

6.128 The Commission considers that this exception is too broad and ambiguous and should not be included in the draft Bill, particularly as the communication or publication prohibitions apply to information obtained from both the lawful and unlawful use of a surveillance device.<sup>125</sup>

### **Communication or publication in the performance of a duty**

6.129 Section 45(2)(c)(ii) of the *Invasion of Privacy Act 1971* provides that a party to a private conversation who used a listening device to overhear, record, monitor or listen to that conversation does not commit an offence by communicating or

<sup>124</sup> *Invasion of Privacy Act 1971* (Qld) s 45(2)(d). Similar provision is made in the surveillance devices legislation in the Australian Capital Territory and Tasmania: *Listening Devices Act 1992* (ACT) s 5(2)(e); *Listening Devices Act 1991* (Tas) s 10(2)(d). In Western Australia, it is a general requirement of any exception to the communication or publication prohibitions that the communication or publication is made to a person who has, or is believed on reasonable grounds by the person making the communication or publication 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: *Surveillance Devices Act 1998* (WA) s 9(3)(b).

<sup>125</sup> Cf *Invasion of Privacy Act 1971* (Qld) s 45, which applies to a party to a private conversation who used a listening device to overhear, record, monitor or listen to that conversation, which is lawful under the Act: see further [6.55] ff above. There is no equivalent exception in s 44 of the Act, which applies to the communication or publication of a private conversation that is unlawfully listened to.

publishing a record, or statement prepared from the record, if the communication or publication is not more than is reasonably necessary in the performance of a duty of the person making it.

6.130 An exception in similar terms is included in the surveillance devices legislation in Western Australia and South Australia.<sup>126</sup>

6.131 In the parliamentary debates relating to the Western Australian provision, it was observed that the concept of 'duty', and the operation of this exception, is potentially broad and ambiguous.<sup>127</sup> It was explained that the exception would apply to communication or publication to, or by, law enforcement officers in the course of their duty.<sup>128</sup> It has also been held that this exception applies to a person acting under a statutory duty.<sup>129</sup> However, the exception is not expressly limited to law enforcement officers or persons employed by government agencies.<sup>130</sup>

6.132 As explained at [6.61]–[6.63] above, the communication or publication prohibitions in the draft Bill apply to the extent that surveillance information relates to a private conversation, a private activity, the geographical location of an individual, vehicle or other thing, or information that is input into, output from, or stored in, a computer.

6.133 In the Commission's view, ordinarily the communication or publication of such surveillance information should not be permitted without consent, unless it is for a particular purpose that justifies the interference with privacy. Whether communication or publication without consent is permitted should not turn on the particular role or status of a person, but rather on the reasons for the communication or publication. The draft Bill therefore does not include an exception for the

<sup>126</sup> *Surveillance Devices Act 2016* (SA) ss 9(1)(h), 12(2)(e); *Surveillance Devices Act 1998* (WA) s 9(2)(a)(v), (3)(a)(ii). In Western Australia, the communication or publication prohibition does not apply if the publication or communication is made 'in the course of the duty of the person making the publication or communication', but the publication or communication must be not more than is reasonably necessary in the performance of the person's duty. In South Australia, it is not an offence to communicate or publish information or material derived from the use of a surveillance device in contravention of the surveillance devices legislation, or in circumstances where the device was used to protect the lawful interests of a person, if the communication or publication is made 'otherwise in the course of duty' or as required or authorised by law.

<sup>127</sup> Western Australia, *Parliamentary Debates*, Legislative Assembly, 17 September 1998, 1675 (J Kobelke).

<sup>128</sup> *Ibid*, K Prince also observing that:

The classic example is law enforcement organisations engaged, perhaps, in a drugs operation, one of which has a form of surveillance on an individual from which it gains information which all those organisations share.

<sup>129</sup> See *Ex parte De Costa* [2014] WASC 454. In this case, an officer investigating an application for a liquor licence came into possession of a recording of a private conversation supporting the inference that the applicant was acting on behalf of another person who had previously been found not to be a fit and proper person to hold a liquor licence. It was held that the officer could provide the recording to a delegate of the Director of Liquor Licensing for the purpose of determining the application for a liquor licence; communication or publication in the course of a person's duty pursuant to s 9(2)(a)(v) of the *Surveillance Devices Act 1998* (WA) includes a statutory duty imposed on a public officer of a State government department to make a report to the Director's delegate in relation to an application for a liquor licence.

It was also noted that communication or publication is permitted in the public interest. However, in Western Australia, there is no general exception for communication or publication in the public interest; a court order is required: *Surveillance Devices Act 1998* (WA) ss 9(2)(viii), 31. It was unnecessary to make an application for an order allowing communication in the public interest in this case, as it was authorised by s 9(2)(a)(v), (which provides an exception for communication or publication in the course of a person's duty).

<sup>130</sup> Western Australia, *Parliamentary Debates*, Legislative Assembly, 17 September 1998, 1675 (J Kobelke and K Prince).

communication or publication of surveillance information in the performance of a duty.

6.134 The communication or publication of surveillance information by public officers in the course of performing their statutory functions, should be captured by one of the other exceptions under the draft Bill, including if the communication or publication is reasonably necessary in the public interest or is authorised under another Act.

6.135 If the communication or publication of surveillance information in particular circumstances, or for a particular purpose, is not adequately addressed by the existing exceptions, it is preferable for that communication or publication to be specifically authorised by other legislation or included as a prescribed circumstance in which the communication or publication is not an offence.

### **Communication or publication by a person who obtained knowledge other than by unlawful use of the device**

6.136 The *Invasion of Privacy Act 1971* contains two separate communication or publication prohibitions. Section 44 applies to the communication or publication of private conversations where the conversation was unlawfully listened to. Section 45 applies to the communication or publication of a private conversation by a party to the conversation who lawfully used a listening device to overhear, record, monitor or listen to that conversation.<sup>131</sup>

6.137 Section 44(2)(b) qualifies the scope of the communication or publication prohibition for *unlawfully* obtained information. It states that the prohibition does not prevent a person from communicating or publishing knowledge of the conversation that is obtained in a manner other than by 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.<sup>132</sup>

6.138 The communication or publication prohibitions in the draft Bill apply to surveillance information obtained from both the lawful and unlawful use of a surveillance device.<sup>133</sup> A provision in similar terms to section 44(2)(b) of the *Invasion of Privacy Act 1971* is therefore not included in the draft Bill.

### **Communication or publication to a party**

6.139 In Queensland and other jurisdictions, surveillance devices legislation provides generally that the communication or publication of information obtained from the use of a surveillance device is not an offence if the communication or publication is made by a party to a private conversation or activity to another party,

<sup>131</sup> See further [6.7] ff and [6.55] ff above.

<sup>132</sup> *Invasion of Privacy Act 1971* (Qld) s 44(2)(b). Similar provision is included in some other jurisdictions, if the communication or publication prohibition applies to information obtained from the *unlawful* use of a surveillance device: *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).

<sup>133</sup> See [6.55]–[6.57] above.

or by a person to another person who was a party to the relevant conversation or activity.<sup>134</sup>

6.140 The communication or publication of surveillance information should be permitted only if it is with consent, or for a particular purpose that justifies the interference with privacy. If a person was a party to a conversation or activity, was tracked or was the owner or lawful controller of a vehicle, computer or other thing, that person would often already have the relevant information. However, communication of a report or record of that information would still represent an interference with privacy, particularly in circumstances where a surveillance device was used without consent.

6.141 The draft Bill therefore does not include an exception for the communication or publication of surveillance information to a party to a private conversation or private activity, a person who was tracked, or the owner or lawful controller of a vehicle, computer or other thing.

## RECOMMENDATIONS

### Communicating or publishing surveillance information

**6-1 The draft Bill should provide that a person must not communicate or publish surveillance information about a private conversation or private activity if the person:**

- (a) knows, or ought reasonably to know, the information is surveillance information; and**
- (b) the person does not have the consent of each party to the conversation or activity to communicate or publish the information.**

*[See Surveillance Devices Bill 2020 cl 28 and [6.60]–[6.66] ff above.]*

**6-2 The draft Bill should provide that a person must not communicate or publish surveillance information about the geographical location of an individual, a vehicle or another thing if the person:**

- (a) knows, or ought reasonably to know, the information is surveillance information; and**
- (b) the person does not have the consent of the following person or persons to communicate or publish the location:**

<sup>134</sup>

*Listening Devices Act 1992 (ACT)* ss 5(2)(a), (6)(2)(a); *Surveillance Devices Act 2007 (NSW)* s 11(2)(a)(i); *Invasion of Privacy Act 1971 (Qld)* ss 44(2)(a)(i), 45(2)(a); *Surveillance Devices Act 2016 (SA)* ss 9(1)(a), 12(2)(a); *Listening Devices Act 1991 (Tas)* ss 9(2)(a)(i), 10(2)(a); *Surveillance Devices Act 1998 (WA)* s 9(2)(a)(i). Further, in New South Wales, a person does not commit an offence if they communicate or publish information regarding the input of information into, or the output of information from, a computer to the person having lawful possession or lawful control of the computer: *Surveillance Devices Act 2007 (NSW)* s 14(2)(a)(i).

- (i) for information about the location of an individual—that individual;
- (ii) for information about the location of the vehicle or other thing—each person who owns, or is in lawful control of, the vehicle or thing.

*[See Surveillance Devices Bill 2020 cl 29 and [6.60]–[6.66] ff above.]*

**6-3** The draft Bill should provide that a person must not communicate or publish surveillance information about information that is input into, output from or stored in a computer, if the person:

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) the person does not have the consent of each person who owns, or is in lawful control of, the computer to communicate or publish the information.

*[See Surveillance Devices Bill 2020 cl 30 and [6.60]–[6.66] ff above.]*

**6-4** The draft Bill should provide that a person who contravenes a prohibition in Recommendations 6-1 to 6-3 above commits an offence, which is punishable by a maximum penalty of 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cll 28, 29 and 30 and [6.68] above.]*

#### **Exceptions to the communication or publication prohibitions**

**6-5** The draft Bill should provide that a person does not commit an offence against the prohibitions in Recommendations 6-1 to 6-3 above if the communication or publication of surveillance information is:

- (a) in a legal proceeding; or
- (b) reasonably necessary to protect the lawful interests of:
  - (i) the person who is making the communication or publication; or
  - (ii) another person who has authorised the person making the communication or publication to do so on their behalf; or
- (c) reasonably necessary in the public interest; or
- (d) reasonably necessary to lessen or prevent a serious threat:

- (i) to the life, health, safety or wellbeing of an individual; or
- (ii) of substantial damage to property; or
- (e) authorised under another Act of the State or an Act of the Commonwealth; or
- (f) in circumstances prescribed by regulation.

*[See Surveillance Devices Bill 2020 cl 31(1) and [6.73] ff above.]*

- 6-6** The draft Bill should provide that a person does not commit an offence against the prohibitions in Recommendations 6-1 to 6-3 above if the use of a surveillance device to obtain the surveillance information the subject of the communication or publication was authorised under another Act of the State or an Act of the Commonwealth.

*[See Surveillance Devices Bill 2020 cl 31(2) and [6.116] ff above.]*

- 6-7** The draft Bill should provide that, for deciding whether the communication or publication of surveillance information is ‘reasonably necessary in the public interest’ for Recommendation 6-5(c) above, a court must consider the following matters as they existed when the person communicated or published the information:

- (a) the subject matter of the surveillance information;
- (b) the scope of the communication or publication;
- (c) the nature of the public interest that arose in the circumstances;
- (d) whether the public interest could have been served in another reasonable way;
- (e) the extent to which the communication or publication affected, or was likely to affect, the privacy of an individual; and
- (f) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

*[See Surveillance Devices Bill 2020 cl 31(3) and [6.105] ff above.]*





# Chapter 7

## Ancillary Matters

INTRODUCTION .....	171
OTHER PROHIBITIONS .....	171
Possession of records obtained from the prohibited use of surveillance devices .....	171
Possession, manufacture, supply or advertising of surveillance devices .....	173
Submissions .....	174
The Commission's view .....	175
USE OF A SURVEILLANCE DEVICE TO HARRASS, INTIMIDATE OR HINDER A PERSON .....	176
Submissions .....	178
The Commission's view .....	179
UNLAWFUL ENTRY OF DWELLING HOUSES .....	180
The Commission's view .....	181
CORPORATE OFFICER LIABILITY .....	181
Submissions .....	182
The Commission's view .....	183
ADMISSIBILITY OF EVIDENCE OBTAINED FROM THE UNLAWFUL USE OF A SURVEILLANCE DEVICE .....	183
Submissions .....	186
The Commission's view .....	186
NON-PUBLICATION ORDERS .....	187
The Commission's view .....	189
FORFEITURE ORDERS .....	190
Submissions .....	191
The Commission's view .....	191
RECOMMENDATIONS .....	192

### INTRODUCTION

7.1 This chapter deals with other matters that are ancillary to the use prohibitions and the communication or publication prohibitions, as well as other issues that were raised in the Consultation Paper and considered in the review.

### OTHER PROHIBITIONS

7.2 Surveillance devices legislation in some jurisdictions includes other ancillary prohibitions, including provisions that make it an offence to:

- possess records obtained from the prohibited use of a surveillance device; or
- possess, manufacture, supply or advertise surveillance devices.

### Possession of records obtained from the prohibited use of surveillance devices

7.3 In the Australian Capital Territory and Tasmania, a person commits an offence under the surveillance devices legislation if the person possesses a record

of a private conversation that the person knows was obtained, directly or indirectly, as a result of the use of a listening device in contravention of the use prohibitions.<sup>1</sup>

7.4 In New South Wales, a person must not possess a record of a private conversation or the carrying on of an activity knowing that it has been obtained, directly or indirectly, by the use of a listening device, an optical surveillance device or a tracking device in contravention of the legislation.<sup>2</sup>

7.5 That provision repealed and replaced a similar provision in section 8 of the *Listening Devices Act 1984* (NSW), with modifications to extend it to cover surveillance devices generally. It was explained, in relation to the earlier provision, that its purpose is:<sup>3</sup>

to fill the significant gap that would be left in the law if it could not successfully prosecute those who have committed a serious offence and effectively destroyed all evidence of its commission, save for the possession of the very thing the crime intended to obtain—that is to say, the private information disclosed in the conversation.

7.6 In each of those jurisdictions, the offence does not apply if the record is in the possession of the person:<sup>4</sup>

- in connection with proceedings for an offence against the legislation;
- with the consent of each principal party to the private conversation or, in New South Wales, each person who took part in the activity; or
- as a consequence of a communication or publication of the record to that person in circumstances that do not constitute an offence against the legislation.

7.7 In Western Australia, the possession of reports or records obtained through the use of a surveillance device is dealt with in the regulations.<sup>5</sup>

7.8 In the Australian Capital Territory, New South Wales and Tasmania, the maximum penalty for the offence is the same as for the use prohibitions and the communication or publication prohibitions.<sup>6</sup> In Western Australia, the penalty does

<sup>1</sup> *Listening Devices Act 1992* (ACT) s 7(1); *Listening Devices Act 1991* (Tas) s 11(1). In Tasmania, the offence also applies if the person knows that the record has been obtained as a result of the unintentional hearing of a private conversation.

<sup>2</sup> *Surveillance Devices Act 2007* (NSW) s 12(1). The offences relates to a contravention of pt 2 of that Act, which contains the use prohibitions and the communication or publication prohibitions.

<sup>3</sup> NSW, *Parliamentary Debates*, Legislative Assembly, 17 May 1984, 1094 (D Landa, Attorney-General).

<sup>4</sup> *Listening Devices Act 1992* (ACT) s 7(2); *Surveillance Devices Act 2007* (NSW) s 12(2); *Listening Devices Act 1991* (Tas) s 11(2).

<sup>5</sup> *Surveillance Devices Regulations 1999* (WA) r 9.

<sup>6</sup> Different maximum penalties for this offence apply in the Australian Capital Territory (50 penalty units (\$8000) or six months imprisonment or both); New South Wales (100 penalty units (\$11 000) or five years imprisonment or both); and Tasmania (40 penalty units (\$6720) or two years imprisonment or both): *Listening Devices Act 1992* (ACT) s 7(1); *Surveillance Devices Act 2007* (NSW) s 12(1); *Listening Devices Act 1991* (Tas) s 12.

not include a term of imprisonment, unlike the use and communication or publication prohibitions.<sup>7</sup>

### Possession, manufacture, supply or advertising of surveillance devices

7.9 Surveillance devices legislation in some jurisdictions makes it an offence to:<sup>8</sup>

- 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;<sup>9</sup>
- 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;<sup>10</sup> or
- advertise a listening device of a prescribed class or description.<sup>11</sup>

7.10 These offences extend the reach of the legislation beyond those who use a surveillance device unlawfully, or who receive, communicate or publish unlawfully obtained information. They reach ‘upstream’ to prohibit activities in ways that may assist in reducing or preventing the ‘downstream’ offences that begin with unlawful use.

7.11 However, the diversity and ubiquity of many multi-purpose technologies that are capable of being used as surveillance devices—including smartphones, drones and other smart devices and programs—makes it difficult to determine upstream actions based on the intended use or design of the device.

7.12 The NZLC observed 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

<sup>7</sup> In Western Australia the penalty is \$5000: *Surveillance Devices Regulations 1999* (WA) r 9(1). The maximum penalty for an offence under the use and communication or publication prohibitions is \$5000 or 12 months imprisonment or both: ss 5(1), 6(1), 7(1), 9(1).

<sup>8</sup> It is also an offence under the *Criminal Code Act 1995* (Cth) if a person manufactures, advertises, displays or offers for sale, sells, or possesses an interception device. An interception device is an apparatus or device that is capable of being used to enable a person to intercept a communication passing over a telecommunications system and could reasonably be regarded as having been designed for the purpose of being used in connection with the interception of communications passing over a telecommunications system: ss 473.1 (definition of ‘interception device’), 474.4.

<sup>9</sup> 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 to be a declared class or kind.

<sup>10</sup> 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 the sale or distribution of a surveillance device, and offers to sell or distribute a surveillance device.

<sup>11</sup> See *Invasion of Privacy Act 1971* (Qld) s 48. This offence is punishable on summary conviction, and has a maximum penalty of 20 penalty units (\$2669) or one year’s imprisonment. No devices have been prescribed for the purpose of this offence.

and restricted to cases in which a person is clearly aiding or encouraging the commission of a crime'. It observed, for example, that:<sup>12</sup>

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.

## Submissions

7.13 In the Consultation Paper, the Commission asked if it is necessary for the legislation to include any other ancillary prohibitions to deal with:<sup>13</sup>

- the possession of records obtained from the prohibited use of surveillance devices; or
- the possession, manufacture, supply or advertising of surveillance devices.

7.14 Some respondents submitted that the legislation should prohibit the possession of records obtained from the prohibited use of a surveillance device.<sup>14</sup>

7.15 A few of those respondents also submitted that the legislation should prohibit the possession, manufacture, supply or advertising of a surveillance device.<sup>15</sup>

7.16 However, the QCCL submitted that those provisions should be limited to circumstances where the possession of records, or the manufacture, supply or advertising of an unlawful surveillance device, 'occurs deliberately or with reckless indifference to the legislation'.

7.17 A few respondents submitted that the legislation should not deal with the possession, manufacture, supply or advertising of a surveillance device.<sup>16</sup> A government department observed that offences should relate to the use of a surveillance device, rather than possession.<sup>17</sup>

---

<sup>12</sup> 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 that can convert a device into a surveillance device, knowing that the device 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: [3.104], Rec 16.

<sup>13</sup> QLRC Consultation Paper No 77 (2018) Q-24.

<sup>14</sup> Eg, Submissions 13, 18, 22, 40.

<sup>15</sup> Submissions 13, 40.

<sup>16</sup> Submissions 15, 18.

<sup>17</sup> Submission 15.

7.18 A community legal service observed generally that there is no need to regulate all ancillary matters. It submitted that the legislation should focus on the most serious issues.<sup>18</sup>

## **The Commission's view**

### ***Possession of records obtained from the prohibited use of surveillance devices***

7.19 The *Invasion of Privacy Act 1971* does not currently prohibit the possession of records obtained from the unlawful use of a listening device. However, surveillance devices legislation in some other jurisdictions does include such an offence.<sup>19</sup>

7.20 The Commission is of the view that the draft Bill should provide an additional privacy protection, by prohibiting a person from possessing information that they know is surveillance information that has been obtained from the unlawful use of a surveillance device. The purpose of such a provision is to reduce the risk of unlawfully obtained surveillance information being communicated or published.

7.21 As previously explained, the draft Bill defines 'surveillance information' as 'information obtained, directly or indirectly, using a surveillance device', and defines 'information' to include a record in any form and a document.<sup>20</sup>

7.22 Accordingly, the draft Bill provides that a person must not, without the consent of each relevant person, possess information that the person knows is surveillance information obtained in contravention of the use prohibitions under the legislation.

7.23 For the purposes of this offence, the draft Bill defines a 'relevant person', in relation to surveillance information, as:<sup>21</sup>

- if the surveillance information is about a private conversation obtained using a listening device—each party to the conversation; or
- if the surveillance information is about a private activity obtained using an optical surveillance device—each party to the activity; or
- if the surveillance information is about the geographical location of an individual obtained using a tracking device—the individual; or
- if the surveillance information is about the geographical location of a vehicle or other thing obtained using a tracking device—each person who owns, or is in lawful control of, the vehicle or thing; or
- if the surveillance information is about the information input into, output from or stored in a computer obtained using a data surveillance device—each person who owns, or is in lawful control of, the computer.

---

18 Submission 41.

19 See [7.3] ff above.

20 See [4.52] above.

21 See further [5.204] ff above in relation to consent to the use of a surveillance device.

7.24 However, the draft Bill provides that a person does not commit an offence if the person is in possession of the information:

- in relation to proceedings for an offence against the legislation; or
- because it was communicated to the person, or published, in a way that does not contravene the legislation.

7.25 The draft Bill provides that the maximum penalty for a contravention of the prohibition on possessing surveillance information is 20 penalty units (\$2669) or one year's imprisonment. For a corporation, the maximum penalty that may be imposed is 100 penalty units (\$13 345).<sup>22</sup>

### **Possession, manufacture, supply or advertising of surveillance devices**

7.26 The Commission considers that the draft Bill should not include prohibitions in relation to possessing, manufacturing, supplying or advertising a surveillance device. Such provisions have limited utility, given that many common devices are capable of being used for the purposes of surveillance.

## **USE OF A SURVEILLANCE DEVICE TO HARRASS, INTIMIDATE OR HINDER A PERSON**

7.27 In Victoria, in the context of its review considering, among other things, 'whether legislative or other measures are necessary to ensure that there is appropriate control of surveillance', the VLRC suggested that the surveillance devices legislation should include an additional offence of a different kind, relating to harassment and intimidation.

7.28 The VLRC recommended the creation of a new offence in the *Surveillance Devices Act 1999* (Vic) to make it unlawful to use a surveillance device in such a way as to:<sup>23</sup>

- (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.

7.29 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, people being filmed while entering abortion clinics, gay bars or drug treatment clinics to

<sup>22</sup> If a body corporate is found guilty of the offence, the court may impose a maximum fine of an amount equal to five times the maximum fine for an individual: *Penalties and Sentences Act 1992* (Qld) s 181B. See [2.39] above.

<sup>23</sup> 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.

intimidate them or hinder their passage, and to the potential use of surveillance for blackmail.<sup>24</sup>

7.30 The VLRC observed that the protection offered by the Victorian Act is generally limited to private conversations and activities and that there are existing laws 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.<sup>25</sup>

7.31 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.<sup>26</sup>

7.32 In Queensland, there are a number of laws of general application that could apply to situations in which a surveillance device is used to intimidate, demean or harass another person.

7.33 These include Criminal Code offences dealing with unlawful stalking, observations or recordings in breach of privacy and the distribution of intimate images or recordings, as well as computer hacking or misuse offences.<sup>27</sup> For example, ‘unlawful stalking’ can include the use of a surveillance device to track or watch a person, or watch a place where a person lives, works or visits.<sup>28</sup>

7.34 There are also mechanisms for obtaining a domestic violence order under the *Domestic and Family Violence Protection Act 2012*.<sup>29</sup> Examples of domestic violence, within a relevant relationship,<sup>30</sup> include conducting unauthorised surveillance (such as, following or tracking a person, monitoring telephone calls, text

---

24 Ibid [6.94]–[6.101].

25 Ibid [6.105]–[6.106].

26 AAUS and Liberty Victoria Paper (2015) [4.5]. AAUS and Liberty Victoria 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’.

27 See Criminal Code (Qld) ss 223, 227A, 227B, 229A, 408E and ch 33A. See further the discussion of those offences in QLRC Consultation Paper No 77 (2018) [2.117] ff.

28 Criminal Code (Qld) s 359B(c)(i), (iii). ‘Unlawful stalking’ can also include: loitering near or approaching a person or a place where a person lives, works or visits; contacting a person in any way (including by email or ‘through the use of any technology’); giving offensive material to a person, directly or indirectly; leaving offensive material where it will be found by, given to or brought to the attention of, a person; an intimidating, harassing or threatening act against a person (whether or not it involves violence or threats of violence); or an act of violence, or a threat of violence, against any person or the property of any person. See further H Douglas and M Burdon, ‘Legal Responses to Non-Consensual Smartphone Recordings in the Context of Domestic and Family Violence’ (2018) 41(1) *University of New South Wales Law Journal* 157, in which it is explained that non-consensual recording of a partner or ex-partner can be unlawful stalking. Whether the conduct justifies a charge of unlawful stalking will depend on the circumstances of the case.

29 See *Domestic and Family Violence Protection Act 2012* (Qld) pt 3.

30 For the purposes of the *Domestic and Family Violence Protection Act 2012* (Qld), a ‘relevant relationship’ is an intimate personal relationship, a family relationship, or an informal care relationship: s 13. The terms ‘intimate personal relationship’, ‘family relationship’ and ‘informal care relationship’ are also defined: see ss 14, 19, 20.

messages or email) or unlawfully stalking a person.<sup>31</sup> Contravention of a domestic violence order is a criminal offence.<sup>32</sup>

7.35 In addition, there are relevant cyber-harassment laws under the Commonwealth Criminal Code. In particular, it is an offence to use a carriage service to ‘menace, harass or cause offence’.<sup>33</sup> This would apply to conduct amounting to harassment by means of the internet, including posting harassing, intimidating or menacing messages or images on social media.<sup>34</sup>

## Submissions

7.36 In the Consultation Paper, the Commission asked if it is necessary for the legislation to include any other ancillary prohibitions to deal with the use of a surveillance device to intimidate, harass or hinder a person.<sup>35</sup>

7.37 Several respondents, including the QLS, the AAUS and a member of the public submitted that the legislation should deal with the use of surveillance devices to intimidate, harass or hinder a person.<sup>36</sup>

7.38 QAI submitted that it should be an offence to use a surveillance device to intimidate, harass or hinder a person ‘with an aggravated component in circumstances where the person subject to surveillance is particularly vulnerable’, for example, because they are a person with a disability or there is a power imbalance between the parties.

7.39 A few respondents gave examples of the use of surveillance cameras to intimidate, harass or stalk neighbours.<sup>37</sup>

7.40 The Women’s Legal Service Qld submitted that there should be a review of the offence of unlawful stalking in the Criminal Code ‘to ensure it adequately covers’ technology assisted abuse in the context of domestic violence. Technology assisted abuse is the use of technology (such as internet, social media, mobile phones,

<sup>31</sup> *Domestic and Family Violence Protection Act 2012* (Qld) s 8(1), (2)(h)–(i). For the purposes of s 8, unauthorised surveillance, of a person, means the unreasonable monitoring or tracking of the person’s movements, activities or interpersonal associations without the person’s consent, including, for example, by using technology: s 8(5) (definition of ‘unauthorised surveillance’).

<sup>32</sup> *Domestic and Family Violence Protection Act 2012* (Qld) ss 30, 177, 180.

<sup>33</sup> *Criminal Code Act 1995* (Cth), sch, s 474.17. The maximum penalty for this offence is three years imprisonment.

<sup>34</sup> ALRC Report No 123 (2014) [15.38].

In Queensland, the Anti-Cyberbullying Taskforce proposed a package of reforms to address cyberbullying of children and young people. The Taskforce did not consider that further criminal offences about bullying and cyberbullying are required in Queensland, although it did recommend that the Queensland Government advocate for the introduction of a national ‘right to erasure’ or ‘right to be forgotten’ law: Queensland Government, *Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland* (September 2018) 72–75, 78 and Rec 29. Queensland Government accepted all 29 of the Taskforce’s recommendations: Queensland Government, *Queensland Government Response to Adjust our Settings: A community approach to address cyberbullying among children and young people in Queensland* (October 2018).

<sup>35</sup> QLRC Consultation Paper No 77 (2018) Q-24(c).

<sup>36</sup> Eg, Submissions 13, 18, 22, 33, 39, 43.

<sup>37</sup> Eg, Submissions 5, 12, 13, 46.



computers and surveillance devices) to stalk and perpetrate abuse on a person.<sup>38</sup> This includes the use of surveillance devices to spy on a person and the use of tracking devices to follow a person. For example, perpetrators may install listening devices or tracking devices on the victim's car or use tracking applications in their ex-partner's phones 'as a form of control, monitoring and intimidation'.<sup>39</sup>

7.41 In particular, the Women's Legal Service supported updating the definition of 'unlawful stalking' to include the use of a surveillance device for the purpose of:

- overhearing, recording, monitoring or listening to a person;
- observing, monitoring or recording a person;
- accessing, tracking, monitoring or recording information that is input into, output from or stored in a computer or other device (for example, a phone); and
- using a surveillance device for the purpose of determining the geographical location of a person, vehicle or object.

### The Commission's view

7.42 The draft Bill provides for offences in relation to the use of a surveillance device, or the communication or publication of information obtained from the use of a surveillance device.<sup>40</sup> In some cases, the use, communication or publication will involve conduct that is harassing, intimidating or demeaning.

7.43 The draft Bill also provides a civil mechanism for resolving complaints in relation to a contravention of the general obligations not to use a surveillance device, or to communicate or publish surveillance information, in a way that interferes with an individual's surveillance privacy.<sup>41</sup>

7.44 In the Commission's view, the draft Bill should not include a separate provision prohibiting the use of a surveillance device to harass, intimidate or hinder a person. A provision of this nature has a different focus from the criminal prohibitions in the draft Bill, which seek to protect the privacy of individuals from unjustified interference from the use of a surveillance device or the communication or publication of information obtained from such use.

7.45 There are a number of offences in the Criminal Code that deal specifically with conduct that is harassing, intimidating or demeaning. Those offences may apply in situations in which a surveillance device is used to intimidate, demean or harass.<sup>42</sup>

---

<sup>38</sup> See further Domestic Violence Resource Centre Victoria, *Legal Guides* <<https://www.dvrcv.org.au/knowledge-centre/legal-protection-safety/legal-guides>>.

<sup>39</sup> Submission 27.

<sup>40</sup> See generally Chapters 5 and 6 above. It also regulates the possession of information obtained from the unlawful use of a surveillance device: see [7.20] ff above.

<sup>41</sup> See generally Chapters 8 and 9 below.

<sup>42</sup> See [7.32] ff above.

7.46 In its submission, the Women's Legal Service Qld suggested that there should be a review of the offence of unlawful stalking to ensure that it adequately applies to all forms of technology assisted abuse in the context of domestic violence. An examination of the scope and operation of that offence is outside the terms of reference for this review. In terms of the scope of existing laws, the Commission notes that the use of a surveillance device to track or watch a partner or former partner without consent could constitute unlawful stalking. Technology-facilitated stalking and abuse could also be a form of domestic violence, and could be the subject of a domestic violence order.<sup>43</sup>

## UNLAWFUL ENTRY OF DWELLING HOUSES

7.47 The *Invasion of Privacy Act 1971* provides that it is an offence to enter a dwelling house without the consent of lawful occupier (or if there is no person in lawful occupation, the owner)<sup>44</sup> or to gain entry by force, threats, intimidation, deceit or fraudulent means,<sup>45</sup> unless the entry was authorised, justified or excused by law or was made to protect the house or a person inside.<sup>46</sup>

7.48 This provision was intended to provide protection 'from forcible or deceptive entry by private inquiry agents or by repossession agents'.<sup>47</sup> The regulation of private inquiry agents and credit reporting agents, which was previously dealt with under the *Invasion of Privacy Act 1971* (Qld), is now regulated under different legislation.<sup>48</sup> In particular, the *Fair Trading Inspectors Act 2014* (Qld) sets out general provisions for the entry of places by inspectors.<sup>49</sup>

7.49 The *Invasion of Privacy Act 1971* also provides that it is an offence for a person to be found in a dwelling house or the yard of a dwelling house without lawful excuse.<sup>50</sup> The purpose of this provision was to strengthen laws and penalties about

<sup>43</sup> See [7.33]–[7.34] above. The domestic and family violence system was the subject of an extensive review in 2014–2015 and is the subject of ongoing reform in Queensland: see Special Taskforce on Domestic and Family Violence in Queensland, *Not Now, Not Ever: Putting an end to domestic and family violence in Queensland*, Report (February 2015); Qld Government, *Domestic and Family Violence Prevention Strategy 2016–2026* (December 2016).

<sup>44</sup> *Invasion of Privacy Act 1971* (Qld) s 48A(1). Those offences are punishable on summary conviction, and have a maximum penalty of 20 penalty units (\$2669) or one year's imprisonment.

<sup>45</sup> *Invasion of Privacy Act 1971* (Qld) s 48A(1A). This offence is punishable on summary conviction, and has a maximum penalty of 30 penalty units (\$4003.50) or 18 months imprisonment. It applies whether or not the offender has the consent of the owner or person in lawful occupation.

<sup>46</sup> *Invasion of Privacy Act 1971* (Qld) s 48A(2). Entry by threats, intimidation, deceit or fraud is not excused: s 48A(2)(a).

<sup>47</sup> Queensland, *Parliamentary Debates*, Legislative Assembly, 1 April 1976, 3330 (WE Knox, Minister for Justice and Attorney-General).

<sup>48</sup> See *Invasion of Privacy Act 1971* (Qld) pts 2 and 3 (as made), pt 3 omitted by the *Tourism, Racing and Fair Trading (Miscellaneous Provisions) Act 2002* (Qld) pt 12. See now, eg, the *Security Providers Act 1993* (Qld) and *Fair Trading Inspectors Act 2014* (Qld); *Privacy Act 1988* (Cth) pt IIIA.

<sup>49</sup> *Fair Trading Inspectors Act 2014* (Qld) pt 2. Generally, an inspector cannot enter a place, other than a public place or a place of business, unless the person has the consent of the occupier of the place or has power to enter under a warrant.

<sup>50</sup> *Invasion of Privacy Act 1971* (Qld) s 48A(3). This offence is punishable on summary conviction, and has a maximum penalty of 20 penalty units (\$2669) or one year's imprisonment.

prowlers or ‘peeping Toms’.<sup>51</sup> It was noted at the time that this provision ‘overcomes difficulties in obtaining prosecutions because of the problems of interpretation’ of the *Vagrants Gaming and Other Offences Act 1931*.<sup>52</sup> That Act was repealed and a number of offences placed in the *Summary Offences Act 2005* (Qld). The latter Act includes a general offence of trespass.<sup>53</sup>

7.50 More broadly, the *Summary Offences Act 2005* and the Criminal Code include general offences relating to trespass.<sup>54</sup> Further, at common law, 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.<sup>55</sup>

### The Commission’s view

7.51 The main purpose of the draft Bill is to regulate the use of surveillance devices.<sup>56</sup> Accordingly, it does not include an offence provision in relation to the unlawful entry of dwelling houses or yards.

### CORPORATE OFFICER LIABILITY

7.52 The *Invasion of Privacy Act 1971* provides that, if a corporation commits certain offences under the Act, each executive officer of the corporation is taken to have also committed the same offence if the officer authorised or permitted the corporation’s conduct constituting the offence, or was, directly or indirectly, knowingly concerned in the corporation’s conduct.<sup>57</sup>

7.53 For the purposes of this provision, an ‘executive officer’ is defined as a person who is concerned with, or takes part in, the corporation’s management, whether or not the person is a director or is given the name of executive officer.<sup>58</sup>

<sup>51</sup> Queensland, *Parliamentary Debates*, Legislative Assembly, 8 & 9 April 1976, 3614 (WE Knox, Minister for Justice and Attorney-General).

<sup>52</sup> In particular, it was noted that the provision in the *Vagrants, Gaming and Other Offences Act* had for many years been restricted to enclosed yards. The *Invasion of Privacy Act 1971* provision applies to all yards, whether enclosed or not. See Qld, *Parliamentary Debates*, Legislative Assembly, 8 & 9 April 1976, 3614–16.

<sup>53</sup> 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. This offence has a maximum penalty of 20 penalty units (\$2669) or one year’s imprisonment.

<sup>54</sup> See 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. This offence has a maximum penalty of 10 years imprisonment. See also Criminal Code ss 421(2), (3), 427(2) for more serious offences. See also *Summary Offences Act 1995* (Qld) s 11, which makes it an offence for a person to unlawfully enter, or remain in, a dwelling or the yard for a dwelling. This offence has a maximum penalty of 20 penalty units (\$2669) or one year’s imprisonment.

<sup>55</sup> See further [D.47] below.

<sup>56</sup> See generally Chapter 5 above. The draft Bill also regulates the communication or publication, and the possession, of surveillance information: see Chapter 6 and [7.20] ff above.

<sup>57</sup> *Invasion of Privacy Act 1971* (Qld) s 49A(1). 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: 49A(2).

<sup>58</sup> *Invasion of Privacy Act 1971* (Qld) s 49A(4).

7.54 This provision does not affect the liability of the corporation for the offence.<sup>59</sup>

7.55 Corporate officer liability provisions are included in other Australian jurisdictions, although their scope differs.<sup>60</sup> By way of example, the provisions in Tasmania and Western Australia exempt an officer from liability for the corporation's conduct if:<sup>61</sup>

- 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.

## Submissions

7.56 In the Consultation Paper, the Commission asked how the liability of a corporate officer for the contravention of the corporation should be dealt with.<sup>62</sup>

7.57 A few respondents submitted that consideration should be given to making corporate officers liable for a contravention by a corporation.<sup>63</sup>

7.58 However, the QLS submitted that:

The approach taken in relation to liability of corporations or corporate officers should be carefully considered in light of existing offences and existing law. Directors and officers of corporations are subject to a range of obligations both under the *Corporations Act 2001* (Cth) and at common law by virtue of their fiduciary positions. New offences should not be created unless there is a clear gap in the law which is not adequately addressed by existing offences.

7.59 The QLS broadly supported the following view expressed by the Corporations and Markets Advisory Committee in its report on personal liability for corporate fault:<sup>64</sup>

[A]s a general principle, individuals should not be made criminally liable for misconduct by a company except where it can be shown that they have

---

<sup>59</sup> *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).

<sup>60</sup> 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.

<sup>61</sup> *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.

<sup>62</sup> QLRC Consultation Paper No 77 (2018) Q-22.

<sup>63</sup> Eg, Submissions 13, 25.

<sup>64</sup> Australian Government, Corporations and Markets Advisory Committee, *Personal Liability for Corporate Fault*, Report (September 2006) 33.

personally helped in or been privy to that misconduct, that is, where they were accessories...

7.60 Toowoomba Regional Council submitted that there should be disciplinary action for an officer in appropriate cases.

### The Commission's view

7.61 The Commission is of the view that the draft Bill should not include a provision to the effect that, where a corporation has committed an offence under the legislation, each executive officer of the corporation is taken to have committed the same offence. The Commission notes that, ordinarily, a corporate officer should not be made responsible for acts or omissions over which they had no control.<sup>65</sup>

7.62 A corporation may be liable for a contravention of a criminal prohibition under the draft Bill.<sup>66</sup> A corporate officer may also be liable for a contravention of a criminal prohibition if they are personally involved in the conduct or an accessory to it, for example in situations where they knew of the contravention and were in a position to influence the corporation's conduct.<sup>67</sup>

### ADMISSIBILITY OF EVIDENCE OBTAINED FROM THE UNLAWFUL USE OF A SURVEILLANCE DEVICE

7.63 Surveillance devices legislation in the Australian Capital Territory, Queensland and Tasmania includes separate provisions that expressly limit the admissibility of evidence obtained from the *unlawful* use of a surveillance device.

7.64 In Queensland, section 46 of the *Invasion of Privacy Act 1971* 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<sup>68</sup> may not give evidence of that conversation in any civil or criminal proceedings.<sup>69</sup> That evidence is admissible only where:<sup>70</sup>

- 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

<sup>65</sup> See generally Office of Queensland Parliamentary Counsel, *Fundamental Legislative Principles: The OQPC Notebook* (2008) [2.9.10], [3.4.1]–[3.4.2]. See also ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002) [8.6]–[8.12]. The ALRC is currently undertaking a review of the Commonwealth corporate criminal responsibility regime, with a particular focus on the need for effective laws to hold corporations accountable for criminal misconduct: see: ALRC, *Corporate Criminal Responsibility*, Discussion Paper No 87 (November 2019).

<sup>66</sup> The prohibitions apply to a 'person', which includes an individual and a corporation: *Acts Interpretation Act 1954* (Qld) s 36, sch 1 (definition of 'person'). If a corporation is found guilty of an offence, the court may impose a maximum fine of an amount equal to five times the maximum fine for an individual: *Penalties and Sentences Act 1992* (Qld) s 181B.

<sup>67</sup> Criminal Code (Qld) ss 7, 10.

<sup>68</sup> Specifically, the use of a listening device in contravention of s 43 of the *Invasion of Privacy Act 1971* (Qld).

<sup>69</sup> *Invasion of Privacy Act 1971* (Qld) s 46(1).

<sup>70</sup> *Invasion of Privacy Act 1971* (Qld) s 46(2).

- 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.<sup>71</sup>

7.65 Similar provision, although varying in terms and scope, is made in the Australian Capital Territory and Tasmania.<sup>72</sup>

7.66 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.<sup>73</sup>

7.67 Surveillance devices legislation in other jurisdictions does not contain similar provisions about the admissibility of evidence, generally leaving the admissibility of evidence unlawfully obtained to the court’s discretion.<sup>74</sup> In New South Wales, the Northern Territory and Victoria, the surveillance devices legislation expressly provides that it ‘is not intended to limit a discretion that a court has to admit or exclude evidence in any proceeding’.<sup>75</sup>

<sup>71</sup> Part 4 of the *Invasion of Privacy Act 1971* (Qld) deals with listening devices.

<sup>72</sup> *Listening Devices Act 1992* (ACT) s 10; *Listening Devices Act 1991* (Tas) s 14. In those jurisdictions, such evidence is also admissible in a proceeding for a ‘defined offence’ (which includes an offence punishable by imprisonment for life or 10 years or more and certain drug offences) (ACT) or an offence punishable by imprisonment for life or 21 years or more, or a serious narcotics offence (TAS): *Listening Devices Act 1992* (ACT) s 10(2)(d), dictionary (definition of ‘defined offence’); *Listening Devices Act 1991* (Tas) ss 3 (definition of ‘serious narcotics offence’), 14(3)(d). In the ACT, evidence obtained by the use of a listening device for the purpose of protecting the lawful interests of a principal party to a private conversation is also admissible under those provisions: *Listening Devices Act 1992* (ACT) s 10(2)(c).

In determining whether to admit evidence under these provisions, the court is required to take into account various matters including: the public interest in upholding the law; protecting people from illegal or unfair treatment and punishing those guilty of offences; the seriousness of the offence in relation to which the evidence is sought to be admitted; and the nature of the relevant contravention of the surveillance devices legislation.

<sup>73</sup> ACT, Legislative Assembly, *Parliamentary Debates*, 20 August 1992, 1880 (T Connolly, Attorney-General, Minister for Housing and Community Services and Minister for Urban Services).

<sup>74</sup> However, the scope of the communication or publication prohibitions (and, in particular, the extent of the exception for communication or publication in legal proceedings) is also relevant. If legislation expressly prohibits the communication of unlawfully obtained evidence to the court, ‘no question of discretion arises: the evidence cannot be received’: The Hon JD Heydon AC, LexisNexis, *Cross on Evidence*, (at June 2019) [27270], citing *Thomas v Nash* (2010) 107 SASR 309. In some jurisdictions, the communication or publication of information obtained from the unlawful use of a surveillance device is permitted in proceedings for an offence against surveillance devices legislation only: see [6.73] ff above.

In some jurisdictions, there are specific provisions relevant to the admissibility of evidence obtained in connection with 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.

<sup>75</sup> *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’.

7.68 At common law, a court has discretion based on public policy to exclude evidence that has been obtained unlawfully or unfairly.<sup>76</sup>

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.

7.69 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.<sup>77</sup>

7.70 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.<sup>78</sup>

7.71 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.<sup>79</sup> However, this provision was repealed by the current legislation. The NSWLRC observed generally that 'provision exists under the *Evidence Act 1995* (NSW) for the court to exclude improperly or illegally obtained evidence'.<sup>80</sup>

7.72 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 improperly or illegally obtained evidence'.<sup>81</sup>

<sup>76</sup> The Hon JD Heydon AC, LexisNexis Australia, *Cross on Evidence* (at September 2018) [27240], [27245], referring to *Bunning v Cross* (1978) 141 CLR 54, 72 and *R v Ireland* (1970) 126 CLR 321, 334–5. The principle is one of general application and it has been noted that 'although there is little authority on the point, there is no reason why the discretion should not be available in civil cases': *ibid* [27270], referring, among others, to *Miller v Miller* (1978) 141 CLR 269, 277 (Gibbs J).

<sup>77</sup> *Ibid* [27245], referring to *Hilton v Wells* (1985) 157 CLR 57, 77.

<sup>78</sup> *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.

<sup>79</sup> *Listening Devices Act 1984* (NSW) s 13. The *Listening Devices Act 1984* (NSW) was repealed and replaced by the *Surveillance Devices Act 2007* (NSW): *Surveillance Devices Act 2007* (NSW) (as made) s 62.

<sup>80</sup> NSWLRC Issues Paper No 12 (1997) [5.24].

<sup>81</sup> ACT Review (2016) [6.41]. In the context of a recording made to protect a principal party's lawful interests, it was 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': [6.45].

## Submissions

7.73 In the Consultation Paper, the Commission asked how the admissibility of evidence, in court proceedings, of information obtained from the unlawful use of a surveillance device should be dealt with.<sup>82</sup>

7.74 Some respondents, including the QLS, submitted that information obtained from the unlawful use of a surveillance device should not be admissible in legal proceedings.<sup>83</sup> A member of the public observed that this might ‘act as a deterrent to the unlawful use of surveillance devices’.<sup>84</sup>

7.75 However, a number of respondents submitted that the admissibility of information obtained from the unlawful use of surveillance devices should be a matter for the court’s discretion.<sup>85</sup>

7.76 The QCCL observed that the admissibility of unlawfully obtained evidence in proceedings requires a careful balance between two conflicting considerations: excluding it ‘may deny trials the most reliable and relevant evidence’; however, ‘admitting it may be seen as legitimising illicit investigation methods’.<sup>86</sup> It submitted that ‘the decision and discretion to reject evidence must remain with the judiciary’.

## The Commission’s view

7.77 The Commission considered whether the draft Bill should contain a provision in similar terms to section 46 of the *Invasion of Privacy Act 1971*, expressly limiting the admissibility of evidence obtained as a direct or indirect result of the unlawful use of a surveillance device.

7.78 Ultimately, however, the Commission is of the view that questions about the admissibility of such evidence should be a matter for the court’s discretion. As noted above, the fact that the information is obtained in contravention of the legislation may more readily justify the exercise of discretion not to admit evidence.<sup>87</sup>

7.79 Accordingly, the draft Bill does not include a provision expressly limiting the admissibility of evidence obtained from the unlawful use of a surveillance device.

7.80 It is not an offence under the draft Bill for a person to communicate or publish surveillance information in a legal proceeding.<sup>88</sup> However, whether that information is admissible as evidence is subject to the rules of evidence, including the discretion to exclude unlawfully obtained evidence. To make this clear, the draft

---

<sup>82</sup> QLRC Consultation Paper No 77 (2018) Q-20.

<sup>83</sup> Eg, Submissions 13, 18, 43.

<sup>84</sup> Submission 13.

<sup>85</sup> Eg, Submissions 15, 22, 40.

<sup>86</sup> Submission 40, referring to L Byrne, ‘Admission of evidence obtained in breach of privacy laws’ (2007) 78 *Precedent* 21.

<sup>87</sup> See [7.69] above.

<sup>88</sup> See [6.79]–[6.80] above.



Bill expressly provides that it does not affect the power of a court to make a decision about the admissibility of information obtained using a surveillance device as evidence in a proceeding.

## NON-PUBLICATION ORDERS

7.81 Section 46(3) of the *Invasion of Privacy Act 1971* provides that, in any proceedings for an offence against Part 4 of the Act, the court may make an order that forbids the publication of evidence of a private conversation, or any report about that evidence, that has been obtained by the unlawful use of a listening device.<sup>89</sup>

- (3) The court before which any proceedings referred to in subsection (2)(c)<sup>90</sup> are brought may, at any stage of the proceedings and from time to time, make an order forbidding publication of any evidence, or of any report of, or report of the substance, meaning or purport of, any evidence referred to in that subsection.
- (4) Any person who contravenes an order made under subsection (3) is guilty of an offence against this Act.

Maximum penalty—10 penalty units. (note added)

7.82 Similar provision, although varying in terms and scope, is made in the surveillance devices legislation in the Australian Capital Territory and Tasmania.<sup>91</sup>

7.83 The starting point in considering whether to include a provision of this kind in the draft Bill is the recognition of the fundamental common law principle of open justice. Court proceedings are ordinarily to take place in open court.<sup>92</sup> The open justice principle also extends to the fair and accurate reporting of proceedings, including the names of the parties and witnesses, and the evidence, testimonial, documentary or physical, that has been given in the proceedings.<sup>93</sup>

7.84 However, the open justice principle is not absolute.<sup>94</sup> There are circumstances where a court may make a non-publication order—at common law in

<sup>89</sup> Part 4 of the *Invasion of Privacy Act 1971* (Qld) contains the use prohibition and the communication or publication prohibitions. Under that Act, evidence of a private conversation that has come to a person's knowledge as a result of the unlawful use of a listening device is inadmissible, except in limited circumstances, including in proceedings for an offence against pt 4 of the Act: see [7.64] ff above.

<sup>90</sup> The proceedings referred to in the *Invasion of Privacy Act 1971* (Qld) s 46(2)(c) are: 'any proceedings for an offence against this Act constituted by a contravention of, or a failure to comply with, any provision of [pt 4] of the Act.'

<sup>91</sup> *Listening Devices Act 1992* (ACT) s 10(5)–(6); *Listening Devices Act 1991* (Tas) s 14(5)–(6).

<sup>92</sup> *Hogan v Hinch* (2011) 243 CLR 506, [20] (French CJ); *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 476 (McHugh JA; Glass JA agreeing at 467). As to proceedings of the Magistrates Courts: see *Justices Act 1886* (Qld) s 70; *Magistrates Courts Act 1921* (Qld) s 14A(1). See also *Human Rights Act 2019* (Qld) s 31(1).

<sup>93</sup> *Hogan v Hinch* (2011) 243 CLR 506, [22] (French CJ); *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 476–77 (McHugh JA; Glass JA agreeing at 467).

<sup>94</sup> See *John Fairfax Publications Pty Ltd v Ryde Local Court* (2005) 62 NSWLR 512, 521 (Spigelman CJ; Mason P and Beazley JA agreeing at 533): 'The "principle of open justice" is a *principle*, it is not a freestanding right' (emphasis in original). See also *Hogan v Hinch* (2011) 243 CLR 506, [20]–[21] (French CJ); *Human Rights Act 2019* (Qld) s 31(2).

the inherent jurisdiction of the Supreme Court or by statute under an express statutory power or in the implied jurisdiction of a statutory court.<sup>95</sup>

7.85 Proceedings for offences under the draft Bill will be summary proceedings under the *Justices Act 1886*, and will fall within the jurisdiction of the Magistrates Courts.<sup>96</sup> Under the *Criminal Practice Rules 1999*, a Magistrate may make an order as a trial judge that he or she considers appropriate about the production at trial, custody or disposal of an exhibit or document marked for identification, and a person may apply to the trial judge for an order allowing the copying of an exhibit for the purpose of publication.<sup>97</sup> Those rules do not expressly deal with other evidence given during a proceeding for an offence.

7.86 The Magistrates Courts do not have the inherent jurisdiction of a Supreme Court to make a non-publication order.<sup>98</sup> But they have the implied power to make orders necessary for the proper administration of justice in exercising their statutory jurisdiction.<sup>99</sup> That is:<sup>100</sup>

an order of a court prohibiting the publication of evidence is only valid if it is really necessary to secure the proper administration of justice in proceedings before it. Moreover, an order prohibiting publication of evidence must be clear in its terms and do no more than is necessary to achieve the due administration of justice. The making of the order must also be reasonably necessary; and there must be some material before the court upon which it can reasonably reach the

<sup>95</sup> *Hogan v Hinch* (2011) 243 CLR 506, [21] (French CJ); *John Fairfax Group Pty Ltd (rec and mgr apptd) v Local Court of New South Wales* (1991) 26 NSWLR 131, 159–60 (Mahoney JA); *R v McGrath* [2002] 1 Qd R 520, [8] (Thomas, Williams JJA and Dutney J), citing *Ex parte The Queensland Law Society Inc* [1984] 1 Qd R 166, 170 (McPherson J).

<sup>96</sup> See *Acts Interpretation Act 1954* (Qld) s 44(1), (2)(d), (4); *Criminal Code* (Qld) s 3(4); *Magistrates Act 1991* (Qld) s 8.

<sup>97</sup> *Criminal Practice Rules 1999* (Qld) rr 55, 56A. In deciding whether to make an order permitting the copying for publication of an exhibit, the trial judge may have regard to a number of matters (under r 56A(4)), including:

- whether it is in the public interest or another legitimate interest;
- the nature of the proposed publication;
- the nature and content of the exhibit and whether it contains private, confidential or personally or commercially sensitive information;
- whether it is likely to prejudice the fair trial of an accused person; and
- the likely effect on a victim of the offence, a family member of the victim or accused person, a person referred to in the exhibit or a person whose personal, proprietary or commercial interests may be affected by the copying for publication; and
- whether the exhibit was produced in open court.

<sup>98</sup> Cf the position of superior courts, which may make non-publication orders in the exercise of their inherent jurisdiction: see *Scott v Scott* [1913] AC 417; *Hogan v Hinch* (2011) 243 CLR 506, [21], [26] (French CJ); *John Fairfax Group Pty Ltd (rec and mgr apptd) v Local Court of New South Wales* (1991) 26 NSWLR 131, 159 (Mahoney JA); *Brooks v Easther* [2017] TASSC 44 (Holt AsJ); *Brooks v Easther (No 2)* [2017] TASSC 47 (Blow CJ).

<sup>99</sup> Inferior courts have implied power to do whatever is necessary within their jurisdiction and to regulate their own proceedings. See *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 476–77 (McHugh JA; Glass JA agreeing at 467); *John Fairfax Group Pty Ltd (rec and mgr apptd) v Local Court of New South Wales* (1991) 26 NSWLR 131, 160–61 (Mahoney JA; Hope AJA agreeing at 169); *John Fairfax Publications Pty Ltd v District Court of New South Wales* (2004) 61 NSWLR 344, [38]–[48] (Spigelman CJ); *Police v Baden-Clay* [2013] QMC 6, [22] (Judge Butler SC, Chief Magistrate).

<sup>100</sup> *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 476–77 (McHugh JA; Glass JA agreeing at 467).

conclusion that it is necessary to make an order prohibiting publication. Mere belief that the order is necessary is insufficient. When the court is an inferior court, the order must do no more than is 'necessary to enable it to act effectively within' its jurisdiction.

7.87 Whether the court will have an implied power to make a non-publication order will depend on the particular circumstances.<sup>101</sup> It has been held that the basis for implying such a power is that:<sup>102</sup>

if the kind of order proposed is not made, the result will be—or at least will be assumed to be—that particular consequences will flow, that those consequences are unacceptable, and that therefore the power to make orders which will prevent them is to be implied as necessary to the proper function of the court. ...[For example,] there will be hardship on the informer or the security officer or the blackmail victim; the future supply of information from such persons will end or will be impeded; and it will be more difficult to obtain from such persons the evidence necessary to bring offenders before the courts and deal with them.

7.88 Apart from any implied power, the court may have an express power under statute to make a non-publication order, as is currently provided in section 46(3) of the *Invasion of Privacy Act 1971*.<sup>103</sup> In Queensland, there are other subject-specific statutory provisions that prohibit the publication of information about proceedings, unless the court orders otherwise.<sup>104</sup>

### The Commission's view

7.89 A fundamental purpose of the draft Bill is to protect an individual's privacy from unjustified interference in particular circumstances. Publication in a court proceeding of information which has been obtained in contravention of the Bill's protections can operate in some circumstances to further the unjustified interference. The Commission considers that there will be cases in which the non-publication of evidence given in a proceeding for an offence is appropriate in the proper administration of justice. This may be particularly the case where the individual concerned is a child or vulnerable person.

7.90 Given the particular context and subject matter of the criminal prohibitions provided for in Part 2 of the draft Bill, the Commission considers that express provision should be included in the draft Bill to empower the making of a non-publication order. This continues the approach taken under the *Invasion of Privacy Act 1971* in relation to criminal offences under that Act.

7.91 The draft Bill accordingly provides that, at any time during a proceeding for an offence against Part 2 of the legislation, the court may make an order prohibiting

<sup>101</sup> An implied power would not be found if its exercise would be inconsistent with the court's statutory obligations: see, eg, *Higgins v Comans* (2005) 153 A Crim R 565.

<sup>102</sup> *John Fairfax Group Pty Ltd (rec and mgr apptd) v Local Court of New South Wales* (1991) 26 NSWLR 131, 160–61 (Mahoney JA; Hope AJA agreeing at 169).

<sup>103</sup> See also, eg, *Legal Profession Act 2007* (Qld) ss 650, 656D, which enables orders to be made prohibiting the publication of information in disciplinary proceedings; and *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 66, which enables QCAT to make a non-publication order in certain circumstances.

<sup>104</sup> See, eg, *Criminal Law (Sexual Offences) Act 1978* (Qld) s 6; *Child Protection Act 1999* (Qld) s 99ZG; *Domestic and Family Violence Protection Act 2012* (Qld) s 159.

the publication of evidence given before the court, other than in the way and to the persons stated in the order. It also provides that such an order may be made only if the court considers it is necessary in the interests of justice.

7.92 The draft Bill further provides that a person must not contravene a non-publication order, unless the person has a reasonable excuse. The maximum penalty for a contravention of this provision is 60 penalty units (\$8007) or three years imprisonment. This is consistent with the maximum penalties for a contravention of a communication or publication prohibition under the draft Bill.

## FORFEITURE ORDERS

7.93 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.

7.94 If the court convicts a person of an offence relating to the unlawful use of a listening device, the court may 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').<sup>105</sup> If the person does not comply, police are empowered to seize the listening device.<sup>106</sup>

7.95 With the exception of Victoria, the surveillance devices legislation in the other Australian jurisdictions also provides for the court to make forfeiture orders upon conviction for an offence. In some jurisdictions, the court may also order the forfeiture or destruction of the record made by the device.<sup>107</sup>

7.96 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:<sup>108</sup>

- 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.

7.97 Before making such an order, the court may give notice to and hear the persons it considers appropriate. A forfeiture order may be made in addition to any penalty imposed for the offence.<sup>109</sup>

<sup>105</sup> *Invasion of Privacy Act 1971* (Qld) s 43(4). This offence is punishable on summary conviction, and has a maximum penalty of 20 penalty units (\$2669): ss 43(5), 49(5).

<sup>106</sup> *Invasion of Privacy Act 1971* (Qld) s 43(6). This applies whether or not proceedings for an offence have started.

<sup>107</sup> *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.

<sup>108</sup> *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'.

<sup>109</sup> *Surveillance Devices Act* (NT) s 73(2), (3).

## Submissions

7.98 In the Consultation Paper, the Commission asked if there should be power to order the forfeiture of a surveillance device used in contravention of the legislation, or of a report or record of information obtained by the use of a surveillance device in contravention of the legislation.<sup>110</sup>

7.99 Several respondents submitted that the legislation should include a power to make forfeiture orders.<sup>111</sup> An academic observed that:<sup>112</sup>

a court should be empowered to order forfeiture of surveillance devices and any records or recordings produced as a result of the use of such devices. The power to order forfeiture of the device should be available particularly where there is actual or a high likelihood of repetition of the behaviour or where there are aggravating factors...

7.100 A community legal service expressed general support for a power of forfeiture, but observed that:<sup>113</sup>

the forfeiture of motor vehicles regime for hooning and other offences has given rise to some problematic issues around ownership and forfeiture of valuable assets.

7.101 It therefore submitted that consideration should be given to the inclusion of defences, particularly around knowledge and consent to use.

7.102 However, Future Wise observed that:<sup>114</sup>

Forfeiture... is fruitless, [in circumstances] where data may already be disseminated and aggregated elsewhere.

7.103 QAI submitted that reports or records should be required to be provided and destroyed and an undertaking required to be provided not to unlawfully use the surveillance device.

## The Commission's view

7.104 The Commission recognises that devices capable of being used as a surveillance device, such as computers and smartphones, are used in contexts that fall outside the scope of the draft Bill. However, in appropriate circumstances, the court should have the power to order the forfeiture of a surveillance device used in connection with the commission of an offence under the legislation.

7.105 The court should also have the power to order the forfeiture of other relevant devices or things, such as a USB device on which the record of a private

---

<sup>110</sup> QLRC Consultation Paper No 77 (2018) Q-23.

<sup>111</sup> Eg, Submissions 13, 15, 18, 19, 40.

<sup>112</sup> Submission 19.

<sup>113</sup> Submission 41.

<sup>114</sup> Submission 25.

conversation or private activity is stored. In addition, the court should have the power to order the forfeiture or destruction of any original or copy of the record.

7.106 Accordingly, the draft Bill provides that, if a person is convicted of an offence against the legislation, the court before which the person is convicted may make an order that:

- a surveillance device used in connection with the commission of the offence is forfeited to the State; or
- a document, device or other thing that contains related information, or on which related information is stored, is forfeited to the State; or
- related information be destroyed.

7.107 The draft Bill defines 'related information' to mean, for an offence, information to which the offence relates, or obtained using a surveillance device to which the offence relates. 'Information' is defined to include a record in any form and a document. Related information therefore includes a record about a private conversation or private activity.

7.108 The draft Bill also provides that:

- before making an order for forfeiture or destruction, the court may require notice to be given to, and hear from, a person the court considers appropriate;
- the power to order forfeiture or destruction applies whether or not the surveillance device, document, device or thing to be forfeited, or related information to be destroyed, has been seized;
- the court may also make any order that it considers appropriate to enforce the forfeiture;
- the provision does not limit the court's powers under the *Penalties and Sentences Act 1992*, the *Criminal Proceeds Confiscation Act 2002* or another law; and
- when forfeited to the State, the surveillance device, document, device or thing becomes the State's property and may be dealt with as directed by the chief executive.

## RECOMMENDATIONS

### **Possessing surveillance information**

- 7-1 **The draft Bill should provide that a person must not, without the consent of each relevant person, possess information that the person knows is surveillance information obtained in contravention of the use prohibitions in the legislation.**

*[See Surveillance Devices Bill 2020 cl 27(1) and [7.20]–[7.22] above.]*

**7-2** For the purposes of the offence in Recommendation 7-1 above, a ‘relevant person’, in relation to surveillance information, means—

- (a) if the surveillance information is about a private conversation obtained using a listening device—each party to the conversation;
- (b) if the surveillance information is about a private activity obtained using an optical surveillance device—each party to the activity;
- (c) if the surveillance information is about the geographical location of an individual obtained using a tracking device—the individual;
- (d) if the surveillance information is about the geographical location of a vehicle or other thing obtained using a tracking device—each person who owns, or is in lawful control of, the vehicle or thing; or
- (e) if the surveillance information is about the information input into, output from or stored in a computer obtained using a data surveillance device—each person who owns, or is in lawful control of, the computer.

*[See Surveillance Devices Bill 2020 cl 27(3) and [7.23] above.]*

**7-3** However, for the purposes of the offence in Recommendation 7-1 above, a person does not commit an offence if the person possesses the information:

- (a) in relation to proceedings for an offence against the legislation; or
- (b) because it was communicated to the person, or published, in a way that does not contravene the legislation.

*[See Surveillance Devices Bill 2020 cl 27(2)) and [7.24] above.]*

**7-4** The draft Bill should provide that the maximum penalty for the offence in Recommendation 7-1 above is 20 penalty units or one year’s imprisonment.

*[See Surveillance Devices Bill 2020 cl 27(1) and [7.25] above.]*

#### **Admissibility of evidence obtained from the use of a surveillance device**

**7-5** The draft Bill should expressly state that it does not affect the power of a court to make a decision about the admissibility of information obtained using a surveillance device as evidence in a proceeding.

*[See Surveillance Devices Bill 2020 cl 4(c) and [7.80] above.]*

**Non-publication orders**

- 7-6** The draft Bill should provide that, in proceedings for an offence against Part 2 of the legislation (which deals with the criminal prohibitions), the court may, at any time during the proceeding and only if it considers it necessary in the interests of justice, make an order prohibiting the publication of evidence given before the court, other than in the way and to the persons stated in the order.

*[See Surveillance Devices Bill 2020 cl 32(1)–(4) and [7.89]–[7.91] above.]*

- 7-7** The draft Bill should provide that a person must not contravene an order made under the provision in Recommendation 7-6 above, unless the person has a reasonable excuse. The maximum penalty for such a contravention is 60 penalty units or three years imprisonment.

*[See Surveillance Devices Bill 2020 cl 32(5) and [7.92] above.]*

**Forfeiture or destruction of surveillance device or information**

- 7-8** The draft Bill should provide that:

- (1)** if a person is convicted of an offence against the legislation, the court before which the person is convicted may make an order that:
  - (a)** a surveillance device used in connection with the commission of the offence is forfeited to the State;
  - (b)** a document, device or other thing that contains related information, or on which related information is stored, is forfeited to the State; or
  - (c)** related information be destroyed;
- (2)** before making an order for forfeiture or destruction, the court may require notice to be given to, and hear from, a person the court considers appropriate;
- (3)** the power to order forfeiture or destruction should apply whether or not the surveillance device, document, device or thing to be forfeited, or related information to be destroyed, has been seized;
- (4)** the court may also make any order that it considers appropriate to enforce the forfeiture;



- (5) the provision in Recommendation 7-8(1) above does not limit the court's powers under the *Penalties and Sentences Act 1992*, the *Criminal Proceeds Confiscation Act 2002* or another law;**
- (6) when forfeited to the State, the surveillance device, document, device or thing becomes the State's property and may be dealt with as directed by the chief executive.**

*[See Surveillance Devices Bill 2020 cl 33(1)–(6) and [7.106], [7.108] above.]*

- 7-9 For the purposes of Recommendation 7-8 above, 'related information', for an offence, should be defined to mean 'information to which the offence relates, or obtained using a surveillance device to which the offence relates'.**

*[See Surveillance Devices Bill 2020 cl 33(7) and [7.107] above.]*



## Chapter 8

# General obligations not to interfere with surveillance privacy of individuals

INTRODUCTION .....	197
SUBMISSIONS .....	197
APPROACHES IN OTHER JURISDICTIONS .....	199
Breach of a criminal prohibition as ground for a civil complaint .....	199
Breach of legislative principles as ground for a civil complaint .....	200
Separate civil ‘tort’ or cause of action .....	202
THE LEGISLATIVE CONTEXT IN QUEENSLAND .....	207
THE COMMISSION’S VIEW .....	207
ELEMENTS OF THE RECOMMENDED APPROACH .....	209
Statement and scope of the general obligations .....	209
Intention and knowledge .....	215
Consent .....	216
Exceptions .....	217
RECOMMENDATIONS .....	225

## INTRODUCTION

8.1 The terms of reference require the Commission to consider appropriate regulation of the use of surveillance devices, including remedies and other appropriate protections for the privacy of individuals.<sup>1</sup>

8.2 There is presently no civil component to surveillance devices legislation. Apart from specific criminal offences, the legislation does not impose any general obligations about the use of a surveillance device in a way that would avoid unjustified interference with an individual’s privacy.

8.3 In the Consultation Paper, the Commission sought submissions about the right to bring a civil proceeding or complaint for contraventions of the surveillance devices legislation.<sup>2</sup>

## SUBMISSIONS

8.4 Many respondents expressed general support for the legislation to include a civil component in addition to the criminal offences. In particular, many respondents expressed support for civil remedies and a complaints mechanism.<sup>3</sup>

---

<sup>1</sup> See terms of reference, paras 1, 5–6 and, in relation to the regulation of the communication or publication of information obtained from the use of surveillance devices, para 2 in Appendix A.

<sup>2</sup> See QLRC Consultation Paper No 77 (2018) Q-25, Q-29(a). See further Chapter 9 below.

<sup>3</sup> Eg, Submissions 13, 15, 18, 19, 33, 38, 39, 40, 41, discussed in Chapter 9 below.

8.5 In this context, most of the respondents referred in general terms to ‘breaches of the legislation’,<sup>4</sup> but a few made more specific submissions.

8.6 An academic submitted that the legislation should provide a civil avenue for dealing with ‘invasions of privacy’ by the use of surveillance devices. In his view:<sup>5</sup>

a shortcoming of the Surveillance Devices Acts in the other jurisdictions is that the various prohibitions are only criminal offences. In no case is there provision for individuals who have had their privacy invaded to obtain civil remedies. By contrast, the Commonwealth *Telecommunications (Interception and Access) Act 1979* provides that the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant remedial relief in respect of the interception of telecommunications and the communication of any record of an intercepted communication, by making such orders against the defendant as the court considers appropriate.<sup>6</sup>

As I have argued elsewhere:

While in a democratic society the state may have an interest in preserving the self-autonomy of its citizens from invasions of their privacy, the value of such prohibitions may depend upon the willingness of the relevant authorities to prosecute transgressions. In any event, it is the individual who has his or her dignity or self-autonomy affronted who has the greater interest in preventing or redressing the wrong.<sup>7</sup>

In the absence of a dedicated cause of action the common law does not provide adequate protection against invasions of privacy. For example, a drone mounted with a [camera] may fly outside of a property line or at a height above that considered to be a height of reasonable [use] for a property and therefore not commit a trespass, but nevertheless still record high definition images in breach of the privacy of those on the property. Further, those images may be disseminated on the internet and thereby lose any quality of confidence, even though they may still constitute an invasion of privacy.

For that reason, Queensland should include in its surveillance devices statute provision for an individual who has had his or her privacy invaded to obtain a civil remedy from the offender. (notes in original)

8.7 Another respondent submitted that there be an avenue ‘to deal with alleged breaches of privacy by either surveillance or other means’.<sup>8</sup>

8.8 Both the OIC and the QCCL submitted that consideration should be given to the introduction in Queensland of a more general statutory ‘tort’ or cause of action for serious invasions of privacy. In their view, this would address any remaining gaps not covered by the surveillance devices legislation. The OIC submitted that:

---

<sup>4</sup> Eg, Submissions 39, 43.

<sup>5</sup> Submission 19.

<sup>6</sup> Section 107A. See also Chapter 9 below.

<sup>7</sup> D Butler, ‘The Dawn of the Age of the Drones: An Australian Privacy Law Perspective’ (2014) 37(2) *UNSW Law Journal* 434, 470.

<sup>8</sup> Submission 29.

Enactment of surveillance devices legislation in Queensland is unlikely to cover every circumstance where privacy invasions have occurred. Criminal penalties are likely to be reserved for the more serious invasions of privacy. While penalties and remedies (if any) under surveillance legislation will form an important part of the privacy protection framework, gaps will remain. The introduction of a statutory cause of action could serve to 'complement the existing legislative based protections afforded to individuals and address some gaps that exist in both common law and legislation'.<sup>9</sup> A statutory cause of action would necessitate the individual taking action, rather than the regulator. (note in original)

8.9 In more general terms, the QLS expressed support for regulation that 'promotes the responsible and reasonable use of surveillance devices'.<sup>10</sup> In its view:

individuals are entitled to a reasonable expectation of privacy, and any surveillance activities—whether in public places or, for example, by use of tracking or location observation or recording—must be appropriately balanced and adequately justified as necessary to the public interest.

QLS shares concerns that inadequately restrained surveillance laws are likely to give rise to an increase in particular privacy risks ... and will have a detrimental effect on the degree to which an individual may be affected by the *intrusive nature, intensity, [and] extended reach* of unrestrained surveillance.<sup>11</sup> (emphasis in original; note added)

## APPROACHES IN OTHER JURISDICTIONS

8.10 The regulation of surveillance devices in Queensland and in the other jurisdictions relies on specific criminal offences that prohibit use, and communication or publication, in particular circumstances.<sup>12</sup>

8.11 Civil approaches to regulation have also been suggested in some jurisdictions.

### Breach of a criminal prohibition as ground for a civil complaint

8.12 One approach is for the contravention of a criminal prohibition in the surveillance devices legislation to also constitute grounds for a civil proceeding or complaint.

8.13 The NSWLRC recommended that the use of surveillance devices for 'covert' surveillance should be regulated through specific authorisation and reporting requirements.<sup>13</sup> It recommended that contravention of any of those requirements

---

<sup>9</sup> Office of the Privacy Commissioner, Submission PR 499 [to the ALRC privacy review], 20 December 2007, cited in ALRC Report No 108 (2008) vol 3, [74.85].

<sup>10</sup> The Insurance Council of Australia similarly submitted that it 'strongly endorse[s] the responsible use of surveillance technology'.

<sup>11</sup> See further QLRC Consultation Paper No 77 (2018) [2.47] in relation to particular privacy risks.

<sup>12</sup> The criminal prohibitions in surveillance devices legislation are discussed in Chapters 5 and 6 above.

<sup>13</sup> See NSWLRC Interim Report No 98 (2001) [2.88]–[2.96], chs 5–6, 8; and [E.2] ff below.

would be a criminal offence, but that it would also enable a person who is aggrieved by the conduct to access a civil complaint process.<sup>14</sup> It noted, in this respect, that:<sup>15</sup>

Since surveillance is an area where both public and private rights may be infringed, it should be possible for a private action to lie concurrently with a prosecution for a criminal offence. Hence, a person aggrieved by conduct infringing covert surveillance legislation should have access to the complaints and review processes ...

8.14 The ALRC made a similar recommendation for surveillance devices legislation to include a civil avenue for redress for 'an individual who has been the subject of unlawful surveillance', where a criminal prohibition is contravened.<sup>16</sup> Such an approach is taken under the *Telecommunications (Interception and Access) Act 1979* (Cth).<sup>17</sup>

### **Breach of legislative principles as ground for a civil complaint**

8.15 Another approach is for surveillance devices legislation to include a set of legislative principles that are enforceable through a civil complaint process.

8.16 The NSWLRC recommended that, in relation to 'overt' surveillance, the legislation should require surveillance users to comply with a set of 'overt surveillance principles' and, in some cases, to formulate a code of practice consistent with those principles.<sup>18</sup> Non-compliance with the principles, or with the requirement to adopt a code of practice, would give rise to liability under a civil complaint process.<sup>19</sup> Overt surveillance would not be regulated by any criminal offences.

8.17 Two of the legislative principles recommended by the NSWLRC were that:<sup>20</sup>

Overt surveillance must only be undertaken for an acceptable purpose [and]

Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.

8.18 As to the first of those principles, the NSWLRC considered that an acceptable purpose for overt surveillance is the protection of a person or property (such as to deter or detect theft, assault or vandalism) or the protection of the public

<sup>14</sup> See NSWLRC Interim Report No 98 (2001) [10.6], [10.11]–[10.14], [10.36]–[10.38], Recs 89, 105. As to the complaints process and remedies proposed by the NSWLRC, see Chapter 9 below.

<sup>15</sup> NSWLRC Interim Report No 98 (2001) [10.38].

<sup>16</sup> ALRC Report No 123 (2014) [14.85], Rec 14-7. See further [9.21]–[9.22] below.

<sup>17</sup> As to the relevant provisions of the *Telecommunications (Interception and Access) Act 1979* (Cth), see [D.2] ff below.

<sup>18</sup> See NSWLRC Interim Report No 98 (2001) [4.32]–[4.37], [4.38]–[4.66], Recs 17, 19; NSWLRC Report No 108 (2005) Rec 1.

<sup>19</sup> NSWLRC Interim Report No 98 (2001) [4.20], [4.32], [10.10], [10.25]–[10.35], Recs 17, 88, 91. As to the complaints process and remedies proposed by the NSWLRC, see Chapter 9 below.

<sup>20</sup> NSWLRC Interim Report No 98 (2001) [4.41]–[4.46]; NSWLRC Report No 108 (2005) [4.10]–[4.27], Rec 1.

interest or a legitimate interest (such as road safety, coastal surveillance or, in some cases, investigative journalism):<sup>21</sup>

Protection of the person and property are relatively straightforward. Protection of the public interest and protection of a legitimate interest are broader categories, created so as not to exclude overt surveillance for another socially acceptable purpose.

8.19 As to the second of the principles above, the NSWLRC explained that the 'reasonable expectation of privacy' test is an 'intuitive measure of the acceptability of surveillance conduct'.<sup>22</sup> In its view:<sup>23</sup>

[This concept] is an acknowledgment of the flexibility required to accommodate different circumstances, including the nature of the surveillance device, the surveillance subject, the location, the occasion and so on. ... [L]egislation such as that being here proposed is designed to maintain an expectation of privacy by restraining unwarranted intrusions by surveillance devices into personal privacy, and thus helping to prevent daily life becoming a surveillance free-for-all.

8.20 The VLRC also recommended that the surveillance devices legislation should include a set of legislative principles. The principles would provide guidance about the 'responsible use of public place surveillance', but non-compliance would not give rise to civil (or criminal) liability.<sup>24</sup>

8.21 Like the NSWLRC, the VLRC's principles referred to the need for public place surveillance to be for a 'legitimate purpose', and to consider individuals' 'reasonable expectations of privacy'.<sup>25</sup> The VLRC stated that '[t]here is increasing international acceptance of the fact that people's reasonable expectations of privacy [can] extend to activities in public places'.<sup>26</sup> It also explained that 'the extent and reasonableness' of people's expectations of privacy differ according to context. In its view:<sup>27</sup>

the reasonableness of any expectation of privacy in public will depend on, among other things, the following factors:

<sup>21</sup> NSWLRC Interim Report No 98 (2001) [4.46], and see [3.7]–[3.19], [4.44]–[4.45]. See also NSWLRC Report No 108 (2005) [4.21]–[4.27].

<sup>22</sup> NSWLRC Interim Report No 98 (2001) [4.41]; and see [4.42] as to factors to consider in determining whether a person has a reasonable expectation of privacy, including the nature or customary use of the location and the timing of the surveillance.

<sup>23</sup> NSWLRC Report No 108 (2005) [4.10], [4.20].

<sup>24</sup> VLRC Report No 18 (2010) [5.1], [5.10], [5.11]–[5.17], Rec 2. The 'public place surveillance principles' would also inform the proposed regulator's functions in encouraging responsible practice, for example, by promoting understanding of best practice and publishing best practice guidelines: [5.2], [5.41]–[5.94], Rec 4(a)–(f), (h). As to the functions of the regulator proposed by the VLRC, see Chapter 10 below.

<sup>25</sup> VLRC Report No 18 (2010) [5.11]–[5.17], [5.21]–[5.24], Rec 2(1), (2), (4). As to a 'legitimate purpose', the VLRC referred with approval to the NSWLRC's categories of acceptable purposes, and additionally considered that the purpose must be related to the activities of the organisation carrying out the surveillance.

<sup>26</sup> Ibid [5.11] and [5.12]–[5.14], citing European and Canadian human rights jurisprudence, common law cases in the United Kingdom and United States of America, the views of other law reform bodies, and views in consultation in its review.

<sup>27</sup> Ibid [5.15].

- a. the location
- b. the nature of the activity being observed
- c. whether the activity is recorded and disseminated
- d. the type of surveillance used
- e. the identity of the person being observed (for example a public official, celebrity or a member of the public)
- f. whether the surveillance was harassing in nature
- g. whether the surveillance was covert
- h. whether the person specifically consented to the surveillance. (note omitted)

### Separate civil ‘tort’ or cause of action

8.22 A different approach—proposed within the wider context of privacy law—is for the introduction of a general statutory ‘tort’ or cause of action for serious invasions of privacy. This would operate as a separate provision, not dependent on a criminal offence.

8.23 A general statutory tort would apply to invasions of privacy by any means. It would therefore apply far more broadly than in the particular context of surveillance devices legislation with which this review is concerned.<sup>28</sup> However, provisions and proposals of this kind provide some guidance on how a limited context civil provision in the surveillance devices legislation might be framed.

8.24 The introduction of a statutory cause of action for invasion of privacy has been recommended by the ALRC, NSWLRC and VLRC (although not implemented).<sup>29</sup> Civil causes of action of this kind have also been adopted, recognised or proposed in some overseas jurisdictions.<sup>30</sup>

8.25 Whilst there are differences in their precise scope and operation, such causes of action have a number of common features. In summary:

<sup>28</sup> See also ACT Review (2016) [7.1]–[7.2] in which it is observed that 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.

<sup>29</sup> ALRC Report No 123 (2014) pt 2; NSWLRC Report No 120 (2009); VLRC Report No 18 (2010) Recs 22 to 24. See also recommendations to adopt the ALRC’s proposed statutory tort in Eyes in the Sky Report (2014) Rec 3; NSW Parliamentary Committee Report (2016) Recs 3, 4; ACCC Digital Platforms Final Report (2019) Rec 19; AHRC Discussion Paper (2019) 92, Proposal 4. See also, eg, A Molnar and D Harkin, *The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware* (Deakin University & ACCAN, August 2019) Rec 5. Cf Australian Government Issues Paper: Serious Invasion of Privacy (2011) 22 ff; and Eyes in the Sky Report: Government Response (2016) 8.

<sup>30</sup> See, eg, the Canadian privacy torts in *Privacy Act*, RSBC 1996 c 373; *Privacy Act*, RSNL 1990, c P-22; *The Privacy Act*, RSS 1978, c P-24; *The Privacy Act*, CCSM, c P125; the common law cause of action for misuse of private information recognised in *Campbell v MGN Ltd* [2004] 2 AC 457 and *Murray v Express Newspapers plc* [2009] 1 Ch 481; and the common law tort for invasion of privacy by publication of private facts recognised in *Hosking v Runting* [2005] 1 NZLR 1.



- A distinction is sometimes drawn between two different types of 'invasion', each of which recognises different privacy interests—intrusion upon seclusion (focusing on watching, listening to, recording or monitoring someone's private activities or unwanted physical intrusion into someone's private space), and misuse of private information (focusing on the use or disclosure of someone's private information).<sup>31</sup>
- Some are limited to 'serious'<sup>32</sup> and/or 'highly offensive' invasions of privacy.<sup>33</sup> This is intended to ensure that trivial or minor breaches of privacy 'do not divert attention away from the more significant cases'.<sup>34</sup>
- All are limited by reference to whether the individual concerned has a 'reasonable expectation of privacy', although there are differences in the precise wording of the test.<sup>35</sup> As the ALRC explained, whether the individual has a reasonable expectation of privacy 'is a useful and widely adopted test of what is private, for the purpose of a civil cause of action for invasions of privacy' and 'is preferable to attempting to define "privacy" in the Act as it is notoriously difficult to define'.<sup>36</sup> The NSWLRC similarly expressed the view that:<sup>37</sup>

[this test] most naturally states the general circumstance in which an individual's privacy should be protected both as a matter of language and as a matter of common sense. ... it does not limit the protection of privacy to particular matters and is inherently flexible, a feature that is important in an area that must remain responsive to technological and social change. It is a formula that features, either as the test, or as part of a test, of actionability in constitutional jurisprudence in the United States and Canada; in European human rights law; and in private law cases in England, New Zealand and the United States. (notes omitted)

- All recognise that the question of whether there is a reasonable expectation of privacy (or an actionable cause of action) requires consideration of all the

<sup>31</sup> See, eg, ALRC Report No 123 (2014) [5.1]–[5.9], Rec 5-1; VLRC Report No 18 (2010) [7.126]–[7.133], Recs 22–24. The NSWLRC recommended a general statutory cause of action that does not distinguish between these two types of invasion. It considered that whilst 'information privacy' and 'intrusion on seclusion' would be the most immediate cases to be covered, 'these two contexts cannot be taken as finally determining the boundaries of privacy': NSWLRC Report No 120 (2009) [4.14]. Cf the common law causes of action in the United Kingdom and New Zealand which apply only in relation to publication: see the cases cited at n 30 above.

<sup>32</sup> See ALRC Report No 123 (2014) Rec 8-1; VLRC Report No 18 (2010) Recs 23, 24.

<sup>33</sup> See VLRC Report No 18 (2010) [7.137]–[7.144], Recs 25, 26; and, in relation to the common law action in New Zealand, *Hosking v Runting* [2005] 1 NZLR 1.

<sup>34</sup> VLRC Report No 18 (2010) [7.142]. See also ALRC Report No 123 (2014) [8.6].

<sup>35</sup> See, eg, ALRC Report No 123 (2014) [6.1]–[6.2], [6.5]–[6.18], Rec 6-1; NSWLRC Report No 120 (2009) [5.1]–[5.2], [5.4], App A cl 74(2); VLRC Report No 18 (2010) [7.128], [7.131], Recs 25(a), 26(a); and *Privacy Act*, RSBC 1996 c 373, s 1(2). See also, eg, in relation to common law causes of action, *Campbell v MGN Ltd* [2004] 2 AC 457, [21] (Lord Nicholls), [85] (Lord Hope); *Murray v Express Newspapers Plc* [2009] 1 Ch 481, [35], [39], [41]; *Re JR38* [2016] AC 1131, [87]–[88] (Lord Toulson JSC), [105]–[108] (Lord Clarke JSC); *Hosking v Runting* [2005] 1 NZLR 1, [117] (Gault and Blanchard JJ), [249] (Tipping J).

<sup>36</sup> ALRC Report No 123 (2014) [6.5]–[6.6].

<sup>37</sup> NSWLRC Report No 120 (2009) [5.4]. See also, eg, D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29(2) *Melbourne University Law Review* 339, 370. That author observes that the 'reasonable expectations' test is a flexible one that enables the circumstances of the case to be taken into account whilst having 'one test [that] is able to apply in all cases': 371.

relevant circumstances. A number of factors to which consideration should be given are commonly identified, including:<sup>38</sup>

- The place or location of the activity, such as the plaintiff's home;
  - The nature of the subject matter, including whether it relates to intimate or family matters, health or medical matters, or financial matters, how the private information was held or communicated, and whether the information was already in the public domain;
  - The means used to obtain the information or intrude upon seclusion, including the use of any device or technology;
  - The purpose of the misuse, disclosure or intrusion;
  - The relevant attributes and conduct of the plaintiff, including their age or occupation, whether they were in a position of vulnerability, and whether they invited publicity or manifested a desire for privacy; and
  - The relationship between the plaintiff and the defendant, including whether they were in a domestic or family relationship.
- All recognise that the cause of action does not apply if the individual has given consent.<sup>39</sup>
  - All also recognise that the right to privacy is not absolute and that there are some circumstances which may justify an invasion of privacy including, in particular, an overriding public interest.<sup>40</sup> Various other defences are also recognised.

### ***Civil 'tort' or cause of action for invasions of privacy by surveillance***

8.26 Relevantly for this review, the LRC Ireland proposed the adoption of a statutory cause of action for invasion of privacy *by means of surveillance*.<sup>41</sup>

8.27 The LRC Ireland's review was concerned specifically with privacy in the context of surveillance and the interception of communications. As it explained, its

<sup>38</sup> See, eg, *The Privacy Act*, RSS 1978, c P-24, s 6; *Privacy Act*, RSBC 1996 c 373, s 1(3); ALRC Report No 123 (2014) [6.26]–[6.83], Rec 6-2; NSWLRC Report No 120 (2009) [5.21]–[5.45], App A cl 74(3)(a). See also, eg, in relation to English case law, NA Moreham, 'Unpacking the reasonable expectation of privacy test' (2018) 134 *Law Quarterly Review* 651, 651, 652, 656; R Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) App cl 2(2); and *Murray v Express Newspapers Plc* [2009] 1 Ch 481, [36] approved in *Re JR38* [2016] AC 1131, [88], [98] (Lord Toulson JSC), [113] (Lord Clarke JSC) and *Weller v Associated Newspapers Ltd* [2016] 1 WLR 1541, [30].

<sup>39</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(2)(a); ALRC Report No 123 (2014) Rec 11-4; NSWLRC Report No 120 (2009) [5.46]–[5.53], App A cl 74(4); VLRC Report No 18 (2010) [7.151]–[7.154], Recs 27(a), 28(a).

<sup>40</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(3)(a); ALRC Report No 123 (2014) Rec 9-1; NSWLRC Report No 120 (2009) [5.14]–[5.20], App A cl 74(2); VLRC Report No 18 (2010) [7.170]–[7.187], Recs 27(f), 28(f).

<sup>41</sup> See LRC Ireland Report No 57 (1998) [7.04]–[7.13].

report 'does not cover the entire sweep of privacy but focuses on one discrete aspect, namely the invasion of privacy through surveillance and interception':<sup>42</sup>

In brief, our core recommendation is for the enactment of a civil tort directed against acts of privacy-invasive surveillance in circumstances where a 'reasonable expectation' of privacy exists. ...

Our main ancillary recommendation is for the enactment of a related civil tort directed against the unjustified disclosure through publication or otherwise of information, images, etc., obtained as a result of the tort of unlawful surveillance or harassment. This does not amount to a full privacy law as conventionally understood—a prohibition on the publication of all manner of private material. Rather, the ambit of our ancillary recommendation builds on our main recommendation which is aimed at surveillance and interception. We make provision for a public interest defence to the tort of disclosure of information obtained as a result of unlawful surveillance. (emphasis omitted)

8.28 It explained that, in addition to other privacy interests such as privacy of personal space and information privacy, 'the interest in freedom from surveillance and the interception of one's communications' is a specific category of privacy. It referred to this category as 'freedom from privacy-invasive surveillance (for short, "surveillance privacy")',<sup>43</sup> that is, 'that freedom which a reasonable person in the circumstances of the case is entitled to expect'.<sup>44</sup> It noted that surveillance privacy is 'not separate' from other privacy interests but 'is connected with and is indeed a particular aspect or segment' of those other privacy interests.<sup>45</sup>

8.29 The LRC Ireland acknowledged that the existence and extent of surveillance privacy will depend 'to a very high degree' on the circumstances of the case.<sup>46</sup>

8.30 Accordingly, it framed its recommended cause of action for invasion of privacy by means of surveillance with reference to a 'reasonable expectation' test. It recommended that the legislation should provide that it is a tort for a person to 'invade the privacy of another person by means of surveillance' and that:<sup>47</sup>

In determining ... whether the privacy of a person has been invaded by means of surveillance, the Court shall consider the extent to which that person was reasonably entitled to expect that he or she should not be subjected to such surveillance having regard to all the relevant circumstances ...

8.31 It further considered that the legislation should include the following list of such 'relevant circumstances':<sup>48</sup>

<sup>42</sup> LRC Ireland Report No 57 (1998) [1.1], [1.4]–[1.5]. It also recommended specific criminal prohibitions against surveillance in particular circumstances: [1.6]. See also [2.12]–[2.14] above.

<sup>43</sup> Ibid [2.2.3]–[2.4], [2.10], quoting ALRC Report No 22 (1983) [2.1].

<sup>44</sup> Ibid [2.10].

<sup>45</sup> Ibid [2.5], quoted at [2.14] above.

<sup>46</sup> Ibid [2.10].

<sup>47</sup> Ibid Head 1(3)(i), 2(i).

<sup>48</sup> Ibid Head 1(3)(i)(a)–(g).

- (a) the place where such surveillance occurred;
- (b) the object and occasion of such surveillance;
- (c) the purpose for which material if any obtained by means of such surveillance was intended to be used...;
- (d) the means of surveillance employed and in particular the nature of any device or apparatus used for such surveillance;
- (e) the status or function of that person;
- (f) the conduct of that person ... insofar as it may have amounted to a waiver, in whole or in part, of that person's privacy in respect of the surveillance at issue...; and
- (g) the context of such surveillance, including the relationship, if any, between the person subjected to the surveillance and the person who carried it out.

8.32 It explained that those interpretative provisions are 'not exhaustive':<sup>49</sup>

This is a reflection, first, of the fact that the extent of one's right to privacy will inevitably vary according to what the subject was reasonably entitled to expect in the circumstances of the case. ... The list of factors indicates the potentially variable boundaries of the right to privacy.

...

It is considered better to give general non-exclusive guidelines to the courts for the purposes of interpreting the content and extent of the right of privacy in each case than to attempt to formulate rigid rules.

This is all the more the case when one appreciates that the content of the right of privacy is at least to some extent a matter for assessment in the light of the social customs and mores of the time. These must be allowed to develop through jurisprudence rather than be the subject of an attempt (which would be almost inevitably unsatisfactory) to create a rigid statutory definition of the right of privacy.

8.33 The LRC Ireland also recommended a statutory cause of action for the disclosure of information obtained by means of privacy-invasive surveillance. It considered that to do otherwise would leave 'a fundamental gap' in the legislation 'given that the disclosure of such information is often the very reason for the surveillance'.<sup>50</sup>

8.34 The LRC Ireland recommended particular defences, including consent and publication in the public interest.<sup>51</sup>

---

<sup>49</sup> Ibid 123–4.

<sup>50</sup> Ibid Head 2(iii), 127.

<sup>51</sup> Ibid Ireland Report No 57 (1998) Head 3.

## THE LEGISLATIVE CONTEXT IN QUEENSLAND

8.35 The *Human Rights Act 2019*—which requires public entities to act in a way that is compatible with human rights<sup>52</sup>—recognises the right to ‘privacy and reputation’. In particular, it provides that an individual has the right not to have their privacy unlawfully or arbitrarily ‘interfered with’.<sup>53</sup>

8.36 Like the other rights under that Act, the right to privacy may be subject to reasonable and justifiable limits, having regard, for example, to the nature of the right, the nature and purpose of the limitation, and whether there are ‘any less restrictive and reasonably available ways to achieve the purpose’.<sup>54</sup>

8.37 The Act does not create a standalone cause of action or civil remedy for unlawful interference with privacy. A human rights claim under the Act may, however, be added to another existing cause of action under other legislation.<sup>55</sup>

8.38 As explained elsewhere, there is an avenue for dealing with some breaches of privacy under the IP Act (applying to government agencies and certain other entities in Queensland) and the *Privacy Act 1988* (Cth) (applying to ‘APP entities’).<sup>56</sup> Both of those Acts provide for an affected individual to make a complaint to the relevant regulator about an alleged contravention of the legislation.<sup>57</sup>

## THE COMMISSION'S VIEW

8.39 A significant shortcoming of the current model of surveillance devices legislation in Queensland and the other jurisdictions is the reliance on criminal prohibitions alone.

8.40 To ‘appropriately protect the privacy of individuals in the context of civil surveillance technologies’,<sup>58</sup> there is a need for surveillance devices legislation to provide a more complete framework of regulation.

8.41 The development and use of surveillance devices and technologies will continue to grow. It is important that regulation meets community expectations about the responsible use of surveillance devices and the protection of individuals’ surveillance privacy.

---

<sup>52</sup> *Human Rights Act 2019* (Qld) ss 4(b), 58(1). See also, eg, ss 4(c)–(d), 38, 39 which impose requirements for Bills introduced into Parliament to be tabled with a statement of compatibility with human rights and for the relevant parliamentary committee to consider and report on the compatibility of Bills with human rights.

<sup>53</sup> *Human Rights Act 2019* (Qld) s 25(a). See generally [D.15]–[D.17] below.

<sup>54</sup> *Human Rights Act 2019* (Qld) s 13(1), (2)(a)–(d).

<sup>55</sup> *Human Rights Act 2019* (Qld) s 59. The Act provides for the Human Rights Commission to conciliate complaints about alleged contraventions of the requirement for public entities to act and make decisions in a way that is compatible with human rights, but there is no provision for civil remedies such as compensation: pt 4 div 2. See [9.31] below.

<sup>56</sup> See generally [D.19]–[D.31] below.

<sup>57</sup> See [9.26]–[9.28] and [9.32]–[9.36] below.

<sup>58</sup> See the terms of reference in Appendix A.

8.42 Effective regulation of the use of surveillance devices requires both a criminal law response, where the seriousness of the conduct and the public interest justify the involvement of the State in imposing criminal sanctions; and a civil law response that recognises the effect of surveillance devices on individual privacy and focuses on promoting the responsible and reasonable use of surveillance devices in day-to-day contexts.

8.43 The civil law response has a potentially wider remit than the criminal law response. It should apply where the relevant conduct interferes with surveillance privacy in an unjustified way, even if it does not meet the criminal threshold or does not result in a prosecution or conviction for an offence against the legislation. All uses of a surveillance device should be responsible and avoid unjustified interference with an individual's surveillance privacy. It is not, therefore, sufficient to provide a right to bring a civil proceeding or complaint only where there has been a contravention of a criminal prohibition.

8.44 In the Commission's view, the draft Bill should include separate civil provisions that impose general obligations on all users of surveillance devices. Stated in general terms, they should provide that a person must not use a surveillance device, or communicate or publish surveillance information, in a way that interferes with an individual's surveillance privacy where the individual:<sup>59</sup>

- has a reasonable expectation of surveillance privacy; and
- has not consented to the use of the surveillance device.

8.45 Additional provisions should be included about the matters to be taken into account in deciding whether, in the circumstances, there is a reasonable expectation of surveillance privacy. There should also be provisions for particular exceptions where the use, or the communication or publication, is permitted.

8.46 Contravention of the general obligations would not be a criminal offence,<sup>60</sup> but would constitute the grounds for an individual who is the subject of the alleged contravention to make a complaint (a 'surveillance device complaint') to the proposed new regulator under the provisions the Commission recommends in Chapters 9 and 10 below.<sup>61</sup>

8.47 The obligations are intended to operate as normative provisions. A complaint about an alleged contravention should not require proof of detriment or damage. This is consistent with the approach taken in other rights-based legislation,

---

<sup>59</sup> As to the particular formulation, including of the 'reasonable expectation of surveillance privacy' test, see further [8.61]–[8.71] below.

<sup>60</sup> Although the conduct may, in some cases, also amount to a contravention of one of the specific criminal prohibitions discussed in Chapters 5 and 6 above.

<sup>61</sup> The complaints mechanism the Commission recommends in Chapter 9 below provides for complaints to be made to the proposed new regulator for mediation and referral of unresolved complaints to QCAT for decision, with the tribunal empowered to order remedial relief (including an order that the respondent must not repeat or continue the act or practice, or must pay the complainant a stated amount, up to \$100 000, as compensation).

such as the IP Act and the *Human Rights Act 2019*.<sup>62</sup> The extent of any harm caused by the contravention would be relevant to the mediation of the complaint or, if referred to QCAT, the orders the tribunal might make.

8.48 It is intended that the civil and criminal provisions would operate side by side; neither a civil nor a criminal outcome would depend on, or be precluded by, the other. Accordingly, an individual should be able to make a complaint about an alleged contravention of an obligation whether or not the conduct is being or has also been dealt with as a criminal offence under the legislation. An individual should also be able to report a suspected contravention of the criminal prohibitions at any time.<sup>63</sup> This will ensure a flexible and responsive approach.

8.49 The scope of the obligations should be limited to the specific context of the draft Bill. They are intended as limited context rights that focus on surveillance devices, not general causes of action for invasion of privacy by any means, which would take their scope beyond surveillance devices legislation. They would apply only with respect to conduct that involves the use of, or the communication or publication of information obtained from the use of, a surveillance device within the meaning of the draft Bill. Neither are they intended to be actionable other than through the specific complaints mechanism included in the draft Bill. They are not statutory torts.

8.50 The Commission considers that the inclusion of general obligations in the legislation will help address the gap in existing laws for the protection of privacy by empowering the individuals most affected to seek redress through a civil complaints mechanism.

8.51 The elements of the Commission's recommended approach are outlined below.

## **ELEMENTS OF THE RECOMMENDED APPROACH**

### **Statement and scope of the general obligations**

#### ***Surveillance device and surveillance information***

8.52 The general obligations should be linked to the use of a 'surveillance device' within the meaning of the draft Bill. This will ensure that the scope of the obligations does not go beyond the scope of the draft Bill (or of the terms of reference for this review).

8.53 Accordingly, the provisions in this part of the draft Bill apply with respect to the use of a 'surveillance device', being a listening device, an optical surveillance device, a tracking device or a data surveillance device as defined by the draft Bill.

---

<sup>62</sup> See *Information Privacy Act 2009* (Qld) ch 5; *Human Rights Act 2019* (Qld) pt 4 div 2. See also, eg, *Anti-Discrimination Act 1991* (Qld) ch 7 pt 1 divs 1–3.

<sup>63</sup> Nothing in the draft Bill prevents a person from reporting a suspected crime or making a complaint to police about an alleged contravention of a criminal offence under the legislation.

They also apply to the communication or publication of information obtained from the use of a surveillance device ('surveillance information').<sup>64</sup>

8.54 The same categories and definitions of surveillance devices apply for both the general obligations and the criminal prohibitions.

### ***Interference with surveillance privacy***

8.55 Canadian privacy torts apply to a 'violation' of privacy.<sup>65</sup> The statutory causes of action recommended by the ALRC, NSWLRC, VLRC and the LRC Ireland use the language of an 'invasion of privacy', and some distinguish between 'intrusion upon seclusion' and 'misuse of private information'.

8.56 In the present context, the Commission prefers an approach consistent with the *Human Rights Act 2019*, the *IP Act* and the *Privacy Act 1988* (Cth), which each relevantly use the language of an 'interference' with privacy.<sup>66</sup> That concept is suitable to capture interference with the relevant aspects of privacy, without the need to distinguish between different types of interference or the risk of inadvertently excluding some types of conduct. It should, however, be limited to interference with 'surveillance privacy', rather than to privacy in general.<sup>67</sup>

8.57 As explained in Chapter 2 above, the interest of direct relevance and concern in the present review is the interest in surveillance privacy.<sup>68</sup>

8.58 This does not mean that other privacy interests are irrelevant. As the LRC Ireland noted, surveillance privacy is connected with other privacy interests (such as privacy of personal space and locational privacy).<sup>69</sup> The Commission's approach will ensure, however, that the specific and more limited context of the general obligations in the draft Bill is clear.

8.59 For the purpose of this part of the draft Bill, 'surveillance privacy', of an individual, means:

- in relation to a particular use of a surveillance device—the individual is not the subject of surveillance from that use of a surveillance device; or
- in relation to surveillance information obtained when the individual was the subject of surveillance—the surveillance information is not communicated or published.

<sup>64</sup> Under the draft Bill, 'surveillance information' means information obtained, directly or indirectly, using a surveillance device: see [4.52], Recs 4-9, 4-10 above.

<sup>65</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 1(1).

<sup>66</sup> See *Human Rights Act 2019* (Qld) s 25(a); *Information Privacy Act 2009* (Qld) s 178(a)(i), (iii); *Privacy Act 1988* (Cth) ss 13, 36(1), 52(1)(b)(i), (1A)(a)(i).

<sup>67</sup> See also [8.59], [8.61]–[8.65] below.

<sup>68</sup> See [2.12] and [8.28]–[8.29] above.

<sup>69</sup> See [8.28] above.



**'Seriousness' or 'offensiveness'**

8.60 In the Commission's view, it is unnecessary to additionally require that the interference is 'serious' or 'highly offensive', as provided for in proposed statutory causes of action for invasion of privacy in some other jurisdictions. Whether there is a reasonable expectation of surveillance privacy will include a consideration of the nature and extent of the interference, including the impact it could be expected to have on an individual in those circumstances.<sup>70</sup> An additional (or alternative) test of 'seriousness' or 'offensiveness' on the one hand risks setting the threshold too high, and on the other hand is not a clear objective standard.

***Where there is a reasonable expectation of surveillance privacy***

8.61 In the Commission's view, the general obligations should apply only where the individual has a reasonable expectation of surveillance privacy. This is broadly consistent with approaches in other jurisdictions,<sup>71</sup> but is adapted to the specific context of the surveillance devices legislation—by referring to a reasonable expectation of 'surveillance privacy', rather than of privacy in general.<sup>72</sup> In this respect, it adopts a similar approach to the LRC Ireland's statutory tort.<sup>73</sup>

8.62 The 'reasonable expectation' of privacy concept is widely recognised in other civil contexts as the test for what should relevantly be protected as 'private'.

8.63 The test will incorporate an objective standard, which is necessary to give practical effect to the obligations. It recognises that not all situations will involve a reasonable expectation of surveillance privacy. For example, an individual might not be reasonably entitled to expect freedom from mass visual surveillance of certain activities in a crowded public place, but may be reasonably entitled to expect freedom from targeted audio surveillance of conversations in a secluded location.

8.64 It will not be every expectation of surveillance privacy, however far-fetched or fanciful, that will attract the protection of the provisions but only those that are reasonable in the circumstances.

8.65 This will require a consideration of the facts of each case.<sup>74</sup> In the Commission's view, this appropriately recognises the contextual nature of the relevant inquiry and will ensure that the provisions are flexible enough to adapt to future circumstances, since what is reasonable may change over time.<sup>75</sup>

***Formulation of the test***

8.66 In the United States context, it has been suggested that a test based on the 'expectations' of privacy may carry the danger that, as privacy-invasive behaviours

---

<sup>70</sup> See further [8.72]–[8.74] below.

<sup>71</sup> See [8.25], [8.30] above. See also [8.19] above.

<sup>72</sup> As to 'surveillance privacy' in the context of these provisions, see also [8.57]–[8.59] above.

<sup>73</sup> See [8.26]–[8.30] above.

<sup>74</sup> As to the factors the Commission recommends should be taken into account, see further [8.74] below.

<sup>75</sup> See, eg, *Hosking v Runting* [2005] 1 NZLR 1, [250] (Tipping J).

become more commonplace, people's expectations of privacy will be diminished and, with them, their legal protection.<sup>76</sup>

8.67 However, the 'reasonable expectation' test is intended to apply as a normative, rather than a descriptive, standard.<sup>77</sup> With reference to the English common law action for misuse of private information, for example, one commentator has explained in this regard that:<sup>78</sup>

Whether a claimant has a reasonable expectation of privacy is a normative enquiry into what privacy protection a claimant can expect the law to provide in the situation in question. Concluding that a person has a reasonable expectation of privacy is a shorthand for saying that, subject to any overriding competing interests, the claimant is *entitled* to expect his or her privacy to be protected in the circumstances of the case.

...

Clearly, it should not be the case that once an intrusive practice becomes sufficiently widespread to be 'in no way unusual or unexpected' ... then all rights of privacy in respect of it are automatically lost. If it were, defendants themselves would set the parameters of the legal privacy interest. As courts have made clear, this is not the position in the English misuse of private information action—rather the focus is on what a person *should* be entitled to expect in the circumstances in question. (emphasis in original)

8.68 The ALRC and the NSWLRC expressed a similar view.<sup>79</sup>

8.69 Taking this into account, it has been suggested that the test could be stated more fully, for example, to refer to a 'reasonable expectation of privacy *protection*'<sup>80</sup> or the privacy that the individual was 'reasonably *entitled* to expect' in all of the circumstances.<sup>81</sup>

8.70 In the Commission's view, there is merit in this suggestion in the present context as well. For the avoidance of doubt, the draft Bill includes a provision to the general effect that the reference to a 'reasonable expectation' of surveillance privacy for an individual means that the individual is reasonably entitled to expect surveillance privacy in relation to a particular use of a surveillance device or in relation to surveillance information obtained when the individual was the subject of

<sup>76</sup> See, eg, E Carolan, 'Surveillance and the individual's expectation of privacy under the Fourth Amendment' (2012) 71(2) *Cambridge Law Journal* 250, 253. See also VLRC Consultation Paper No 7 (2009) [3.91]–[3.93].

<sup>77</sup> See, eg, LRC Ireland Report No 57 (1998) [5.5]; NSWLRC Report No 120 (2009) [5.5]; ALRC Report No 123 (2014) [6.7] note 2, citing *R v Tessling* [2004] 3 SCR 432, 443, 447 (Binnie J). See also *Campbell v MGN Ltd* [2004] 2 AC 457, [99] (Lord Hope); *Murray v Express Newspapers Plc* [2009] 1 Ch 481, [35], [39] (Sir Anthony Clarke MR for the Court); *Re JR38* [2016] AC 1131, [98] (Lord Toulson JSC), [109] (Lord Clarke JSC); *Weller v Associated Newspapers Ltd* [2016] 1 WLR 1541, [20]–[21] (Lord Dyson MR; Tomlinson and Bean LJJ agreeing); *Hosking v Runting* [2005] 1 NZLR 1, [250] (Tipping J).

<sup>78</sup> N Moreham, 'Unpacking the reasonable expectation of privacy test' (2018) 134 *Law Quarterly Review* 651, 653–5, citing the English cases in n 77 above.

<sup>79</sup> See ALRC and NSWLRC above n 77.

<sup>80</sup> Moreham, above n 78, 655 (emphasis added).

<sup>81</sup> NSWLRC Report No 120 (2009) [5.4], App A cl 74(2) (emphasis added); LRC Ireland Report No 57 (1998) Head 1(3)(i). And see, eg, *Privacy Act*, RSBC 1996 c 373, s 1(2).

surveillance. This is generally consistent with the approach proposed by the LRC Ireland.<sup>82</sup>

8.71 The reference to a 'reasonable entitlement' will make it clear that the question is not whether the individual subjectively expected that they would not be surveilled, but whether it was reasonable to expect that they *should* not be subject to the surveillance. It also reinforces that the test is an objective one, albeit one that will take into account all the relevant circumstances, including those relating to the individual concerned.

### ***A non-exhaustive list of factors***

8.72 Whether there is a reasonable expectation of surveillance privacy will depend on the particular context. Accordingly, for the purpose of the general obligations, the draft Bill includes a non-exhaustive list of factors that must be considered in deciding whether the individual has a reasonable expectation of surveillance privacy.

8.73 This will help give practical effect to the provisions, and is broadly consistent with approaches in other contexts.<sup>83</sup> Whilst a comprehensive and precise definition of what should be protected from the use of a surveillance device is difficult, it is possible to identify several important factors relevant to the question of whether there is a reasonable expectation of surveillance privacy.

8.74 Accordingly, the draft Bill provides that the matters that are relevant to consider include (but are not limited to) the following:

- The individual's location when the surveillance device is used—this might include consideration, for example, of whether the individual is in their home, in other private premises or in a public place, as well as the nature or customary use of the location, such as a change room;
- The subject matter of the use, or of the surveillance information, including whether it is of an intimate, familial, health-related or financial nature;
- The type of device used;
- The nature and purpose of the use, communication or publication, including:
  - the extent to which the use, communication or publication targets the individual;
  - whether the use is covert;
  - in relation to the communication or publication of surveillance information, how the information is communicated or published; and

---

<sup>82</sup> See [8.29]–[8.30] above.

<sup>83</sup> See [8.19], [8.21], [8.25], [8.31]–[8.32] above.

- whether the use, communication or publication contravenes a provision of an Act;
- the nature and extent of any notice given about the use;
- whether the individual has an opportunity to avoid the surveillance;
- The attributes and conduct of the individual, including:
  - the extent to which the individual has a public profile, invites or encourages publicity or shows a wish for privacy;
  - the extent to which the individual is in a position of vulnerability—this might include consideration, for example, of the individual’s age or other personal circumstances or situation;
  - the nature of any relationship between the individual and the person using the surveillance device or making the communication or publication—for example, whether they are in a domestic or family relationship; and
  - the effect that the use, communication or publication is reasonably likely to have on the individual’s health, safety or wellbeing.

8.75 The list draws on factors identified in other contexts as being relevant to establishing a ‘reasonable expectation of privacy’,<sup>84</sup> but focuses on surveillance privacy. For example, it refers to whether the use of the surveillance device was covert, and the extent of any notice given about the surveillance.

8.76 Some factors may be of greater weight or significance than others in the particular circumstances. There may also be other relevant circumstances not specifically mentioned in the list. The list is non-exhaustive and is not intended to be restrictive.<sup>85</sup>

8.77 With one exception,<sup>86</sup> the listed factors are intended to apply both to the use of a surveillance device, and to the communication or publication of surveillance information. It may be just as relevant in the case of a communication or publication to consider, for example, whether the information is obtained from the use of a surveillance device that is covert, that targets the individual, or that observes or records the individual in their home.

8.78 The listed factors are matters to be considered and weighed in a balancing exercise, not a ‘purely mechanical application of legal principles ... to create an

---

<sup>84</sup> See [8.19], [8.21], [8.25], [8.31]–[8.32] above.

<sup>85</sup> It is a general principle of administrative law that a decision maker must take relevant considerations into account, and must not take irrelevant considerations into account, in making the decision: see, eg, *Judicial Review Act 1991* (Qld) ss 20(2)(e), 21(2)(e), 23(a)–(b).

<sup>86</sup> That is, in relation to communication or publication, how the information is communicated or published.

illogical conclusion'.<sup>87</sup> It is not intended to suggest, for example, that if the individual is located in a public place or has a public profile there can be no reasonable expectation of surveillance privacy. Whilst there may generally be a lower expectation of privacy in such circumstances, it is possible for a reasonable expectation of surveillance privacy to arise in particular situations.

8.79 For example, whether an individual with a public profile has a reasonable expectation of surveillance privacy may depend on whether their activity relates to the exercise of their public functions, is a commonplace personal activity or is of an intimate nature. Distinctions can also be drawn between 'people who are reluctantly or involuntarily put in the public spotlight, such as the victim of a crime, [and] those who seek the limelight'.<sup>88</sup>

8.80 It is also recognised that an individual may have a reasonable expectation of surveillance privacy in a public place. A 'public place' can encompass a variety of locational settings, with differing degrees of public and private expectations.<sup>89</sup> For example, there are some locations, whether or not they might otherwise be classed as 'public' that are 'well-known places of retreat', such as changing rooms and toilet cubicles.<sup>90</sup>

## Intention and knowledge

8.81 The statutory causes of action for invasion of privacy recommended by the ALRC, NSWLRC and VLRC are each intended to apply to both intentional and reckless conduct.<sup>91</sup> This is generally consistent with Canadian privacy torts, which apply to 'wilful' violations of privacy.<sup>92</sup>

8.82 The NSWLRC and VLRC additionally considered that negligent acts should also be capable of being captured.<sup>93</sup> The VLRC explained, for example, that:<sup>94</sup>

Although it is highly likely that most serious invasions of privacy will involve intentional conduct, there may be circumstances in which a person's actions were so grossly negligent that civil action ought to be possible. An example might be a medical practitioner who leaves a patient's highly sensitive medical records on a train or tram.

<sup>87</sup> ALRC Report No 123 (2014) [6.46], quoting *Daily Times Democrat v Graham*, 162 So 2d 474, 478–9 (Ala, 1964) (Harwood J).

<sup>88</sup> See generally ALRC Report No 123 (2014) [6.68], citing *In re S* [2003] 3 WLR 1425 and *Campbell v MGN Ltd* [2004] 2 AC 457, [142] (Baroness Hale). See also, eg, *Hosking v Runting* [2005] 1 NZLR 1, [120]–[124] (Gault and Blanchard JJ).

<sup>89</sup> See generally, eg, VLRC Consultation Paper No 7 (2009) [3.53]–[3.89]; VLRC Report No 18 (2010) [5.11]–[5.14] and the cases cited there.

<sup>90</sup> Moreham, above n 78, 666. See also [3.31] above.

<sup>91</sup> ALRC Report No 123 (2014) [7.2]–[7.5], Rec 7-1 (consistently with its earlier view in ALRC Report No 108 (2008) [74.164]); NSWLRC Report No 120 (2009) [5.56]; VLRC Report No 18 (2010) [7.148].

<sup>92</sup> *Privacy Act*, RSBC 1996 c 373, s 1(1); *Privacy Act*, RSNL 1990, c P-22, s 3(1); *The Privacy Act*, RSS 1978, c P-24, s 2.

<sup>93</sup> See NSWLRC and VLRC at n 91 above.

<sup>94</sup> VLRC Report No 18 (2010) [7.148].

8.83 Alternatively, the statutory privacy tort in Manitoba includes a specific defence where the person, having acted reasonably, ‘neither knew [n]or should reasonably have known that the [conduct] constituting the violation would have violated the privacy of any person’.<sup>95</sup>

8.84 Similar considerations apply in the present context.

8.85 The Commission considers that the general obligations should cover both intentional and negligent conduct and, for this purpose, prefers the approach in Manitoba which has the advantage of simplicity as well as incorporating reasonableness. Accordingly, a person does not contravene the obligations in this part of the draft Bill if the person did not know and ought not reasonably to have known that the use of the surveillance device or, relevantly, the communication or publication, would interfere with the individual’s surveillance privacy.

8.86 In the Commission’s view, this will ensure that intentional interferences are captured, as well as those that an ordinary person would reasonably foresee in the circumstances. A person will not be able to unfairly deny responsibility by asserting that they did not intend the interference if it was a reasonably foreseeable consequence of their actions.

8.87 It will also be broadly consistent in effect with the approach taken to the criminal prohibitions in Chapters 5 and 6 above.<sup>96</sup>

8.88 The Commission considers that the knowledge requirement is an essential element in defining the scope of the obligations and that, accordingly, it would be for the complainant to show that the alleged contravener had the requisite knowledge.

## Consent

8.89 Consistently with the Commission’s view that consent is a key informing concept in the review, the general obligations should not apply if the individual concerned has consented to the relevant conduct.

8.90 Accordingly, the draft Bill provides that a person does not contravene the general obligations if the individual concerned has consented to the use of the surveillance device in that way or, relevantly, to the communication or publication. Consent should be taken to mean express or implied consent, consistently with Recommendation 4-11 above.<sup>97</sup>

8.91 In other civil contexts, consent is an exception, where the onus would be on the defendant.<sup>98</sup> The VLRC considered that ‘[t]o do otherwise is to force the plaintiff

---

<sup>95</sup> *The Privacy Act*, CCSM, c P125, s 5(b).

<sup>96</sup> The Commission recommends that the mental element of the criminal prohibitions be left to the operation of s 23 of the Criminal Code: see [5.126]–[5.132], [6.60] above.

<sup>97</sup> See [4.100] above.

<sup>98</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(2)(a); ALRC Report No 123 (2014) [11.52], [11.68], Rec 11-4; VLRC Report No 18 (2010) [7.154], Recs 27(a), 28(a). See also LRC Ireland Report No 57 (1998) Head 3(1)(i).

to engage in the difficult task of proving a negative'.<sup>99</sup> In contrast, the NSWLRC considered that consent is an essential element of its recommended privacy tort and that the plaintiff should bear the relevant onus.<sup>100</sup>

8.92 In the Commission's view, consent is a key element in defining the scope of the obligations. As such, it would be for the complainant to show that they did not consent. Whilst this would require the complainant to 'prove a negative', the Commission does not consider this to be an unfair burden. It is also consistent with the approach to consent in the criminal prohibitions that the Commission recommends in Chapters 5 and 6 above.

## Exceptions

8.93 There are also other circumstances in which a person should not be taken to have contravened the general obligations. The inclusion of exceptions to the provisions recognises that the right to privacy in relation to the use of surveillance devices is not absolute, and may need to give way to other countervailing rights and interests in appropriate circumstances.

8.94 The Commission considers that, in general terms, the exceptions to the general obligations in this part of the draft Bill should be broadly consistent with those it recommends for the criminal prohibitions. However, the approach should be tailored to the scope and purpose of the general obligations, which are intended to have a potentially wider and more flexible operation.

## Authorised or required by law

8.95 In other contexts, both civil and criminal, an excuse or exception for conduct that is authorised or required by law is commonly recognised. This applies, for example, to offences under the Criminal Code,<sup>101</sup> the use or disclosure of personal information under the *Privacy Act 1988* (Cth) and IP Act,<sup>102</sup> and the statutory privacy torts in Canada.<sup>103</sup>

8.96 The statutory causes of action for invasion of privacy recommended by the ALRC, NSWLRC and VLRC also include such a defence.<sup>104</sup> For example, the

---

<sup>99</sup> VLRC Report No 18 (2010) [7.154].

<sup>100</sup> NSWLRC Report No 120 (2009) [5.51].

<sup>101</sup> See Criminal Code (Qld) s 31(1), which provides that, with some exceptions, a person is not criminally responsible for acts or omissions 'in execution of the law' or required by a lawful order of a competent authority. See also Criminal Code (Cth) s 10.5.

<sup>102</sup> See *Privacy Act 1988* (Cth) sch 1 APP 6.2(b), APP 8.2(c), APP 9.2(c); and *Information Privacy Act 2009* (Qld) sch 3 IPP 10(1)(c), IPP 11(1)(d), sch 4 NPP 2(1)(f), NPP 9(1)(b). Similarly, under the *EU General Data Protection Regulation*, art 6(1)(b)–(c), processing of personal data is lawful if it is necessary for the performance of a contract or compliance with a legal obligation.

<sup>103</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(2)(c) which applies where the act or conduct was authorised or required under a law in force in British Columbia, by a court or by any process of a court.

<sup>104</sup> See ALRC Report No 123 (2014) Rec 11-7; NSWLRC Report No 120 (2009) [6.3], App A cl 75(1)(a); VLRC Report No 18 (2010) [7.159], Recs 27(c), 28(c). See also LRC Ireland Report No 57 (1998) Head 3(1)(ii) in relation to conduct in 'fulfilling a legal duty, or exercising a legal power'.

NSWLRC proposed a defence where the conduct of the defendant was required or authorised:<sup>105</sup>

- by or under a NSW law or Commonwealth law; or
- by an Australian court or tribunal or a process of such a court or tribunal.

8.97 Those Commissions considered this especially important for government agencies in carrying out their functions under other laws.<sup>106</sup>

8.98 The Commission considers that such an exception is also appropriate in the present context.

8.99 The draft Bill accordingly provides that a person does not contravene the general obligations if the use of a surveillance device or, relevantly, the communication or publication of surveillance information is authorised or required by law, or by an order or process of a court or tribunal.

8.100 This is consistent in general terms with the exception to the criminal prohibitions, for conduct ‘authorised under another Act’, that the Commission recommends in Chapters 5 and 6 above.

### ***Incidental to the defence of a person or property***

8.101 In other contexts, an excuse or exception for conduct undertaken in self-defence, in defence of another person or in defence of property is recognised. Depending on the circumstances, it is a defence to an intentional tort to use reasonable force to avert the threat of imminent harm to a person, or to use reasonable means to defend property against an immediate danger.<sup>107</sup> Similar defences apply under the Criminal Code.<sup>108</sup> A key element is that the conduct is reasonably necessary.

8.102 Information privacy legislation also includes specific exceptions of this kind. For example, the IP Act permits the use or disclosure of personal information where

<sup>105</sup> NSWLRC Report No 120 (2009) App A cl 75(1)(a).

<sup>106</sup> ALRC Report No 123 (2014) [11.7]; NSWLRC Report No 120 (2009) [6.3]; VLRC Report No 18 (2010) [7.158].

<sup>107</sup> See generally A Stickey, *Australian Torts Law* (LexisNexis Butterworths, 2016, 4th ed) [6.30]–[6.37]; Westlaw AU, *The Laws of Australia* (online at 3 January 2020) 33 Torts ‘3.39 Defences’.

<sup>108</sup> See, eg, Criminal Code (Qld) ss 271 (self-defence), 273 (defence of another), 277, 278 (defence of property), which apply both to civil and criminal actions for assault: see Stickey, above n 107, [3.37]–[3.45].

See also Criminal Code (Qld) s 31(1)(c)–(d), which provide that, with some exceptions, a person is not criminally responsible for acts ‘reasonably necessary in order to resist actual and unlawful violence’ threatened to the person or to another person in their presence, or, in particular circumstances, for acts or omissions to save the person or another person, or to save their property or the property of another person, from serious harm or detriment.



it is 'necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual'.<sup>109</sup>

8.103 The statutory privacy torts in Canada, and those recommended by the ALRC, NSWLRC and VLRC, provide for a defence where the conduct is incidental to the exercise of a lawful right of defence of person or property.<sup>110</sup> For example, the VLRC proposed a defence, in similar terms to the ALRC, where:<sup>111</sup>

[the] conduct was incidental to the exercise of a lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm ...

8.104 The NSWLRC recommended a similar defence, adding that such conduct might include 'the prosecution or defence of civil or criminal proceedings'.<sup>112</sup>

8.105 The ALRC explained that its proposed provision would apply in circumstances of self-defence, as well as defence of another person and defence of property:<sup>113</sup>

The defence will ... protect individuals from liability where their conduct protects a third party from harm. The conduct is more likely to be considered necessary and reasonable where that third party is under the individual's care or responsibility, such as a member of their family, or where that third party is incapable of exercising self-defence, but the defence would not be limited to such circumstances. At common law, the defence extends to protection of an individual's household, employer, family members and even, in some circumstances, strangers.

The defence would also protect individuals from liability where their conduct was in defence of property, although different weight is given to the defence of property compared with the defence of persons. This is analogous to the defence for intentional torts where a defendant's conduct in response to a threat or harm to their property is reasonable. (notes omitted)

8.106 The Commission considers that a similar exception is appropriate in the present context.

<sup>109</sup> See *Information Privacy Act 2009* (Qld) sch 3 IPP 10(1)(b), IPP 11(1)(c), sch 4 NPP 2(1)(d), NPP 9(1)(c). In some circumstances, the collection, use or disclosure of personal information may also be permitted if it is 'necessary for the establishment, exercise or defence of a legal or equitable claim': see *Information Privacy Act 2009* (Qld) sch 4 NPP 9(1)(d); and *Privacy Act 1988* (Cth) s 16A table item 4, sch 1 APP 3.4(b), APP 6.2(c). Similar provision for the processing of personal data where it is necessary in 'the vital interests' of the data subject is made under the *EU General Data Protection Regulation*, art 6(1)(d).

<sup>110</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(2)(b); *The Privacy Act*, CCSM, c P125, s 5(c); ALRC Report No 123 (2014) Rec 11-2; NSWLRC Report No 120 (2009) [6.2], App A cl 75(1)(b); VLRC Report No 18 (2010) Recs 27(b), 28(b). See also LRC Ireland Report No 57 (1998) Head 3(1)(ii)(a) in relation to conduct 'defending or maintaining a legal right'.

<sup>111</sup> VLRC Report No 18 (2010) Recs 27(b), 28(b); ALRC Report No 123 (2014) Rec 11-2.

<sup>112</sup> NSWLRC Report No 120 (2009) App A cl 75(1)(b), which provides that 'the conduct of the defendant was done for the purpose of lawfully defending or protecting a person or property (including the prosecution or defence of civil or criminal proceedings)'.

<sup>113</sup> ALRC Report No 123 (2014) [11.32], [11.36]–[11.37], citing, for example, R Balkin and J Davis, *Law of Torts* (LexisNexis Butterworths, 5th ed, 2013) [6.17]–[6.18]. The ALRC additionally recommended a defence of necessity which would focus on situations of 'imminent danger or emergency': [11.35], [11.41], Rec 11-3.

8.107 In Chapters 5 and 6 above, the Commission recommends exceptions to the criminal prohibitions for the protection of a relevant person's 'lawful interests', and for obtaining evidence of, or lessening or preventing, a 'serious threat to the life, health, safety or wellbeing of an individual, or substantial damage to property'.<sup>114</sup>

8.108 The exception to the obligations in this part of the draft Bill should encompass aspects of those same concepts. However, the Commission considers that a formulation in more general terms, such as that proposed by the VLRC and the NSWLRC is more appropriate in this context.

8.109 Accordingly, the draft Bill provides that a person does not contravene the general obligations if the use of the surveillance device or, relevantly, the communication or publication of surveillance information is incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property, including to prosecute or defend a civil or criminal proceeding.

8.110 The exception applies where the use, communication or publication is incidental to an action taken in defence of a person or property that is itself lawful. This would incorporate consideration, in accordance with accepted legal principles, of whether the steps taken in defence of the person or property were a reasonable response to an imminent or immediate danger.<sup>115</sup>

8.111 The exception also applies where the use, communication or publication is reasonably necessary for this purpose; this will ensure that more is required than mere convenience or desirability.<sup>116</sup>

### **Public interest**

8.112 The protection of an individual's surveillance privacy may conflict with countervailing public interests, such as the public interest in the detection, investigation or prosecution of crime or the public interest in freedom of political communication. In some circumstances, the countervailing public interest may be of such importance as to override the individual's surveillance privacy.<sup>117</sup>

8.113 The statutory privacy torts in Canada include a defence for the publication of information where 'the matter published was of public interest or was fair comment on a matter of public interest'.<sup>118</sup> The public interest is also included in the statutory

<sup>114</sup> See Recs 5-12, 5-15, 5-16, and 6-5(b), (d) above.

<sup>115</sup> See generally [8.101], [8.105] above and the references cited there.

<sup>116</sup> See also, N Witzleb, 'A statutory cause of action for privacy? A critical appraisal of three recent Australian law reform proposals' (2011) 19 *Torts Law Journal* 104, 127:

If the defence did not contain a reasonableness requirement, it would be open to abuse and fail to give the plaintiff's privacy the protection it deserves in the circumstances of each case.

<sup>117</sup> See further [5.284] ff above as to the meaning of 'public interest'.

<sup>118</sup> See *Privacy Act*, RSBC 1996 c 373, s 2(3)(a); *Privacy Act*, RSNL 1990, c P-22, s 5(2)(a); *The Privacy Act*, RSS 1978, c P-24, s 4(2)(a). The defence does not apply if the manner in which the information was obtained was itself a 'violation' of privacy. See also *The Privacy Act*, CCSM, c P125, s 5(f).

causes of action for invasion of privacy recommended by the ALRC, the NSWLRC and the VLRC.

8.114 The ALRC proposed that, for the individual to have a cause of action, 'the court must be satisfied that the public interest in privacy outweighs any countervailing public interest'. In its view, a balancing exercise is appropriate to ensure that privacy interests are not unduly privileged over other important public interests.<sup>119</sup> The NSWLRC recommended a similar approach.<sup>120</sup>

8.115 In contrast, the VLRC recommended a defence to its proposed causes of action for invasion of privacy if:<sup>121</sup>

[The] conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.

8.116 In its view, the public interest should be a 'limited concept':<sup>122</sup>

not all matters of interest to the public are matters of public interest that ought to deprive a person of their right to privacy. In particular, the public interest defence ought not to extend to matters that satisfy a curiosity about the private lives of others, but serve no other purpose relevant to the common good.

8.117 The LRC Ireland similarly recommended a limited public interest defence, for the disclosure of information obtained by surveillance.<sup>123</sup> Under its proposals, a disclosure would not be in the public interest 'merely because the object of such surveillance, or such information or material, is or would be newsworthy'.<sup>124</sup> It also proposed that the defence would apply only to the extent that the disclosure was not of 'such a nature or degree that it exceeds what was required to satisfy the public interest'.<sup>125</sup> The LRC Ireland explained in this regard that:<sup>126</sup>

[This] is directed to cases where, although publication of information obtained by privacy-invasive surveillance is justified in the public interest, the actual publication effected in the particular case, by reason for example of its extent or detail, goes beyond what is so justified. The public interest defence is not intended as a charter for the gratuitous publication of salacious or otherwise excessive details of people's intimate or private lives going beyond what is reasonably necessary to satisfy the public interest. It is intended solely to enable the public interest (in the sense of the common good) to be served.

119 See ALRC Report No 123 (2014) [9.7], [9.27], [11.147]–[11.148], Rec 9-1.

120 NSWLRC Report No 120 (2009) [5.15], App A cl 74(2).

121 VLRC Report No 18 (2010) [7.170]–[7.187], Recs 27(f), 28(e).

122 Ibid [7.187].

123 LRC Ireland Report No 57 (1998) Head 3(1)(iv). The defence would apply if the disclosure was justified, or the defendant believed on reasonable grounds that it was justified, 'by overriding considerations of the public interest'.

124 Ibid Head 3(2). In its view, the 'public interest' should be limited to matters of 'the common good': 135.

125 Ibid 138, [2.44], Head 3(iv) proviso (b). It also recommended other limitations on the public interest defence, including that the surveillance by which the information was obtained was not a criminal offence.

126 Ibid 138.

8.118 Public interest defences or exceptions are also recognised in other contexts, including under information privacy legislation.<sup>127</sup> For example, an agency's obligation to comply with the privacy principles in the IP Act may be waived or modified if there is an overriding public interest in doing so.<sup>128</sup> In addition, the Act permits the use or disclosure of personal information, by or for a law enforcement agency, if it is necessary for one or more of the following purposes:<sup>129</sup>

- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;
- (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
- (iii) the protection of the public revenue;
- (iv) the prevention, detection, investigation or remedying of seriously improper conduct;
- (iv) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; ...

8.119 In Chapters 5 and 6 above, the Commission recommends exceptions to the criminal prohibitions against use, communication and publication where the use of the surveillance device, or the communication or publication of surveillance information, 'is reasonably necessary in the public interest'.

8.120 The Commission considers that a similar exception is also appropriate in the present context.

8.121 The exception should apply only if the relevant public interest outweighs, in all the circumstances, the individual's surveillance privacy. The Commission considers that, together with the addition of the qualifying words 'reasonably necessary', this will introduce a balancing exercise and ensure that more is required to relieve a person from liability than merely identifying a public interest. In this way, the mere existence of a public interest will not automatically prevail. If there is a less intrusive means of satisfying the public interest, the exception would not operate.

8.122 Taking this approach, the draft Bill provides that a person does not contravene the general obligations if the use of the surveillance device or, relevantly, the communication or publication of surveillance information is reasonably necessary in the public interest and the relevant public interest outweighs the interference with the individual's surveillance privacy.

<sup>127</sup> See also, eg, the public interest defences to racial and religious vilification in the *Anti-Discrimination Act 1991* (Qld) s 124A(2)(c), and to unlawful stalking in the Criminal Code (Qld) s 359D(c).

<sup>128</sup> See *Information Privacy Act 2009* (Qld) s 157(4), discussed at n 77 in Chapter 10 below. See also *Privacy Act 1988* (Cth) s 72 which similarly provides for public interest determinations. Similarly, under the *EU General Data Protection Regulation*, art 6(1)(e), the processing of personal data is lawful if it is necessary for the performance of a task carried out in the public interest.

<sup>129</sup> See *Information Privacy Act 2009* (Qld) sch 3 IPP 10(1)(d), IPP 11(1)(e). A law enforcement agency is defined in sch 5, relevantly, to mean the QPS, the CCC, the department in which the *Corrective Services Act 2006* (Qld) is administered and any other agency to the extent it has particular enforcement functions. Similar exceptions apply under the *Privacy Act 1988* (Cth) sch 1 APP 6.2(e).

8.123 The Commission does not consider it necessary, in light of this formulation, to additionally list any other factors to be considered in determining whether the exception applies. Whether the exception applies will depend on the particular circumstances of each case. The Commission observes that the independent regulator under the draft Bill is empowered to issue guidelines about the exceptions to the obligations, including examples.<sup>130</sup>

8.124 Like the VLRC, the Commission intends that the 'public interest' is to be understood as a limited concept, and not as any matter in which members of the public may be merely interested or curious.

### ***Performance of a duty under a law***

8.125 The VLRC recommended a specific defence to its proposed causes of action for invasion of privacy that would apply to public officers, namely, where:<sup>131</sup>

[The person] is a police or public officer who was engaged in his/her duty and the [person's] conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass ...

8.126 The statutory privacy torts in Canada include a similar defence for law enforcement officers acting in the course of their duties.<sup>132</sup>

8.127 The LRC Ireland also recommended a defence to its proposed statutory cause of action for invasion of privacy by surveillance where the person 'was fulfilling a legal duty' and the surveillance or disclosure 'was justified by and was not disproportionate to the legal interest pursued'.<sup>133</sup> In particular, it considered that this would apply to a member of the police force in obeying a lawful order.<sup>134</sup>

8.128 The Commission does not consider it necessary in the present context to include an additional exception of this kind. Public officers, or others, who are performing their lawful duties will be protected to the extent that the use, communication or publication is 'authorised or required by law' or 'by an order or process of a court or tribunal'.<sup>135</sup> The public interest exception may also apply, for example, if the use, communication or publication is made by a public officer for the protection of members of the public or the safety of a public officer in the performance of their functions.<sup>136</sup> This is consistent with the approach taken to the criminal prohibitions in Chapters 5 and 6 above.

---

<sup>130</sup> See Rec 10-10(d)(ii) below.

<sup>131</sup> VLRC Report No 18 (2010) Recs 27(d), 28(d).

<sup>132</sup> See, eg, *Privacy Act* RSBC 1996 c 373, s 2(2)(d).

<sup>133</sup> LRC Ireland Report No 57 (1998) Head 3(1)(ii).

<sup>134</sup> Ibid 132.

<sup>135</sup> See [8.95]–[8.100] above. See also [4.5]–[4.8] above as to the Commission's view that the draft Bill should not affect the operation of another law regulating the use of surveillance devices.

<sup>136</sup> See [8.112]–[8.124] above.

### ***Exceptions analogous to defamation defences***

8.129 Similar defences to those that apply in the context of defamation also apply, or have been proposed, for statutory causes of action for invasion of privacy by publication. This includes, for example, the defences of absolute privilege, fair report of proceedings of public concern and fair comment on matters of public interest.<sup>137</sup>

8.130 The ALRC proposed that some defamation defences (namely, absolute privilege, fair report of proceedings of public concern and publication of public documents) should be available, but that others (such as truth, qualified privilege, innocent dissemination, and information in the public domain) should not.<sup>138</sup>

8.131 The *Defamation Act 2005* provides the following defences to defamation in addition to the general law:<sup>139</sup>

- justification;
- contextual truth;
- absolute privilege;
- publication of public documents;
- fair report of proceedings of public concern;
- qualified privilege for provision of certain information;
- honest opinion;
- innocent dissemination; and
- triviality.

8.132 The Commission does not recommend any analogous exceptions for the criminal prohibitions against communication or publication in Chapter 6 above.

8.133 The Commission is of the view that, to the extent they may be relevant to the general obligations, these issues are adequately and appropriately covered by the other exceptions it recommends, including the public interest exception. To include additional exceptions based on those available for defamation would unduly widen the available exceptions and undermine the protection conferred by the obligations.

8.134 Defamation has a different focus and protects different interests. The focus of the obligations in this part of the draft Bill is the responsible use of surveillance devices, and the responsible communication or publication of surveillance information, to protect an individual's surveillance privacy. The relevant inquiry is not whether information is, for example, true or trivial, but whether there is a

<sup>137</sup> See, eg, *Privacy Act*, RSBC 1996 c 373, s 2(3); ALRC Report No 123 (2014) [11.82], [11.93]–[11.94], Recs 11-5, 11-7; NSWLRC Report No 120 (2009) [6.6]–[6.10], App A cl 75(1)(c); VLRC Report No 18 (2010) Rec 27(e).

<sup>138</sup> ALRC Report No 123 (2014) [11.89]–[11.90], Rec 11-6; [11.132]–[11.146]. The NSWLRC proposed a defence in similar terms to the 'innocent dissemination' defence to defamation: NSWLRC Report No 120 (2009) App A cl 75(1)(d).

<sup>139</sup> *Defamation Act 2005* (Qld) pt 4 div 2.

countervailing interest that outweighs the interference with the individual's surveillance privacy.

## RECOMMENDATIONS

### **General obligations not to interfere with surveillance privacy of individuals**

**8-1 The draft Bill should include civil provisions, separate from the criminal prohibitions in the legislation, that:**

- (a) impose obligations on the use of, or the communication or publication of information obtained from the use of, a surveillance device, within the meaning of the draft Bill, to avoid interference with an individual's surveillance privacy; and**
- (b) form the basis for the complaints mechanism in Recommendations 9-1 to 9-32 below.**

**The civil provisions should have the features set out below.**

*[See Surveillance Devices Bill 2020 pts 3 and 4, and [8.39] ff above.]*

### **Statement and scope of the general obligations**

**8-2 The draft Bill should provide that, if an individual has a reasonable expectation of surveillance privacy:**

- (a) a person must not use a surveillance device in a way that interferes with the individual's surveillance privacy; and**
- (b) a person must not communicate or publish the surveillance information in a way that interferes with the individual's surveillance privacy.**

*[See Surveillance Devices Bill 2020 cll 36(1)–(2) and 37(1)–(2), and [8.44] above.]*

**8-3 However, a person does not contravene a general obligation in Recommendation 8-2 above if:**

- (a) the individual concerned has consented to the surveillance device being used in that way or, relevantly, to the communication or publication; or**
- (b) the person did not know, and ought not reasonably to have known, that the particular use of the surveillance device or, relevantly, the communication or publication would interfere with the individual's surveillance privacy.**

*[See Surveillance Devices Bill 2020 cll 36(3) and 37(3), and [8.81]–[8.92] above.]*

**8-4 The draft Bill should provide that, for the purpose of this part of the draft Bill:**

- (a) ‘surveillance privacy’, of an individual, means:**
  - (i) in relation to a particular use of a surveillance device—the individual is not the subject of surveillance from that use of a surveillance device; or**
  - (ii) in relation to surveillance information obtained when the individual was the subject of surveillance—the surveillance information is not communicated or published; and**
- (b) ‘reasonable expectation’, of surveillance privacy for an individual, means the individual is reasonably entitled to expect surveillance privacy—**
  - (i) in relation to a particular use of a surveillance device; or,**
  - (ii) in relation to surveillance information obtained when the individual was the subject of surveillance.**

*[See Surveillance Devices Bill 2020 cl 34, and [8.55]–[8.71] above.]*

**8-5 The draft Bill should provide that the matters that are relevant for deciding whether an individual has a reasonable expectation of surveillance privacy include (but are not limited to) the following:**

- (a) the individual’s location when the surveillance device is used;**
- (b) the subject matter of the use, or of the surveillance information, including whether it is of an intimate, familial, health-related or financial nature;**
- (c) the type of device used;**
- (d) the nature and purpose of the use, communication or publication, including:**
  - (i) the extent to which the use, communication or publication targets the individual;**
  - (ii) whether the use is covert;**
  - (iii) in relation to the communication or publication, how the information is communicated or published; and**
  - (iv) whether the use, communication or publication contravenes a provision of an Act;**



- (e) the nature and extent of any notice given about the use;**
- (f) whether the individual has an opportunity to avoid the surveillance;**
- (g) the attributes and conduct of the individual, including:**
  - (i) the extent to which the individual has a public profile, invites or encourages publicity or shows a wish for privacy;**
  - (ii) the extent to which the individual is in a position of vulnerability;**
  - (iii) the nature of any relationship between the individual and the person using the surveillance device, or making the communication or publication; and**
  - (iv) the effect that the use, communication or publication is reasonably likely to have on the individual's health, safety or wellbeing.**

*[See Surveillance Devices Bill 2020 cl 35, and [8.72]–[8.80] above.]*

#### **Exceptions to the general obligations**

**8-6 A person does not contravene a general obligation in Recommendation 8-2 above if the person's use of a surveillance device or, relevantly, communication or publication of surveillance information:**

- (a) is authorised or required by law or by an order or process of a court or tribunal;**
- (b) is incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property, including to prosecute or defend a criminal or civil proceeding; or**
- (c) is reasonably necessary in the public interest and the public interest outweighs the interference with the individual's surveillance privacy.**

*[See Surveillance Devices Bill 2020 cl 38, and [8.93]–[8.134] above.]*



# Chapter 9

## Civil complaints process and remedies

INTRODUCTION .....	229
SUBMISSIONS.....	229
Mediation or conciliation of complaints .....	229
Civil remedies.....	230
EXISTING PROVISIONS AND PROPOSALS .....	233
Other jurisdictions .....	234
Other legislation in Queensland .....	235
THE COMMISSION'S VIEW .....	239
ELEMENTS OF THE RECOMMENDED APPROACH .....	242
Making and referring complaints to the commissioner .....	242
Dealing with complaints .....	246
Mediation of complaints .....	250
Referral of complaints to tribunal .....	253
Enforcement of tribunal orders .....	259
RECOMMENDATIONS .....	260

### INTRODUCTION

9.1 The terms of reference require the Commission to consider appropriate regulatory powers and remedies.<sup>1</sup>

9.2 In the Consultation Paper, the Commission sought submissions on whether the legislation should provide for the conciliation or mediation of complaints by an independent regulator, and whether civil remedies should be available in relation to contraventions of the surveillance devices legislation.<sup>2</sup>

### SUBMISSIONS

#### Mediation or conciliation of complaints

9.3 The majority of respondents who addressed these questions—including the Department of Agriculture and Fisheries, the Department of Education, the Brisbane City Council, the Toowoomba Regional Council, the AAUS, Future Wise, the QCCL, the Townsville Community Legal Service Inc. and the OIC—agreed that there should be provisions to allow complaints about contraventions of the legislation to be made to an independent regulator for mediation or conciliation.<sup>3</sup>

---

<sup>1</sup> See terms of reference, paras 4–5 in Appendix A.

<sup>2</sup> See QLRC Consultation Paper No 77 (2018) Q-25, Q-26, Q-29(a). As to whether there should be an independent regulator, see Q-28 and Chapter 10 below. The Commission also sought submissions about the effect of non-compliance by a respondent with a civil order for relief: at Q-27.

<sup>3</sup> Submissions 10, 13, 15, 18, 19, 22, 25, 33, 35, 38, 39, 40, 41.

9.4 QAI submitted that this would be a ‘preferable first step’ as a cost-effective approach to dealing with contraventions, and noted the importance of ensuring that this is accessible:

We note that there is an imbalance in relation to access to justice that people with a disability experience. Conciliation and mediation, while preferable to litigation, can still be costly and for those on government pensions can be out of reach. A no cost jurisdiction to support enforcement and regulation may offer some reprieve.

9.5 Future Wise similarly submitted that the regulator should be responsible for mediating and conciliating complaints ‘in a cost-effective and accessible way’.<sup>4</sup>

9.6 Some respondents, including the AAUS, the Department of Education and an academic, favoured taking the same approach as the IP Act, so that complaints are first made to an independent regulator for mediation and, if they cannot be mediated, referred to QCAT for decision.<sup>5</sup> The AAUS proposed, for example, that:<sup>6</sup>

A person subject to prohibited conduct under the uniform provisions should have the right to make a complaint to the relevant ... regulator, who may reject, investigate or conciliate the complaint. On request of a complainant, complaints that cannot be conciliated should be determined by the relevant Tribunal.

9.7 The NSW Privacy Commissioner, whilst not expressing a view about whether the legislation should include a complaints mechanism, observed that the most common surveillance complaints received by its office are those involving neighbour disputes about security cameras and videos, and the use of drones by private sector companies or businesses.<sup>7</sup> The Townsville Community Legal Service Inc., which supported a complaints mechanism, noted that the three most common surveillance issues raised by its clients involve surveillance in care and health settings (such as aged care),<sup>8</sup> surveillance where there is interpersonal violence, and surveillance between neighbours.

## Civil remedies

9.8 Most respondents who addressed these questions—including the Department of Agriculture and Fisheries, Toowoomba Regional Council, the AAUS, the QCCL, the QLS, the Townsville Community Legal Service Inc. and QAI—also

---

<sup>4</sup> The importance of accessibility was also noted in Submission 19.

<sup>5</sup> Eg, Submissions 10, 19, 39.

<sup>6</sup> AAUS and Liberty Victoria Paper (2015) [1.2](8), adopted in Submission 39 from the AAUS. In that paper, the AAUS and Liberty Victoria suggested the adoption of uniform, harmonised surveillance devices legislation and the conferral of functions on the state and territory privacy commissioners.

<sup>7</sup> This respondent noted that surveillance complaints also commonly relate to ‘workplace surveillance’. Workplace surveillance is excluded from this review: see terms of reference, para F in Appendix A. It is the subject of a separate reference that has been referred to the Commission.

<sup>8</sup> The issue of surveillance in aged care settings has been raised in evidence and submissions to the Commonwealth’s ongoing Royal Commission into Aged Care Quality and Safety: Royal Commission into Aged Care Quality and Safety, *Interim Report: Neglect* (October, 2019) vol 2, 129, 196, 203, 229. See also, eg, L Martin, ‘Oakden whistleblower calls for surveillance cameras in Australian nursing homes’, *The Guardian* (online), 16 January 2019.

agreed that there should be provision for civil remedies<sup>9</sup> in addition to the criminal offences.<sup>10</sup>

9.9 An academic expressed the view that the approach to civil remedies under the IP Act provides a useful model:<sup>11</sup>

any such remedies [under the surveillance devices legislation] should be easily accessible: it should not only be those with substantial resources and who can afford to commence legal action that are able to obtain civil remedies for invasion of their privacy. In this respect the Queensland laws concerning data protection provide a useful model. The *Information Privacy Act 2009* Chapter 5 provides a process by which privacy complaints may be made. Such complaints are referred to the Information Commissioner, who may in the first instance seek to resolve complaints judged not to be 'frivolous, vexatious, misconceived or lacking in substance' by way of mediation. However, the Commissioner must refer the complaint to QCAT if asked to do so by the complainant. Where QCAT finds that the complaint is substantiated it may ... grant a range of remedies including injunction and monetary compensation

9.10 The OIC also expressed general support for this approach:

The IP Act allows an individual to make a complaint about an agency's breach of the privacy principles. If an individual—who need not be a Queensland citizen—considers that a Queensland government agency has failed to comply with its obligations under the privacy principles, they are able to make a formal complaint to the agency in the first instance, and to the OIC if they are not satisfied by the agency response.

If an accepted complaint cannot be mediated, the complainant can ask OIC to refer the complaint to the Queensland Civil and Administrative Tribunal (QCAT) for its determination and orders. QCAT may make an order restraining the agency from repeating any act or practice, order the agency to carry out certain acts, award compensation to the complainant not exceeding \$100 000 and/or make further orders against the agency.

...

OIC notes there are no civil remedy provisions in the surveillance devices legislation of the other Australian states and territories. OIC supports consistency with privacy laws of other jurisdictions. (notes omitted)

9.11 The AAUS made a similar submission.<sup>12</sup> This respondent submitted that, whilst the relevant regulator should be responsible for handling complaints in the first

<sup>9</sup> Submissions 13, 15, 18, 19, 25, 33, 38, 39, 40, 41, 43.

<sup>10</sup> Eg, Submissions 13, 19, 38, 39, 40. Cf Submission 15 which submitted that civil remedies should be provided in preference to criminal proceedings.

<sup>11</sup> Submission 19. The complaints process under the *Information Privacy Act 2009* (Qld) is outlined at [9.26] ff below.

<sup>12</sup> See AAUS and Liberty Victoria Paper (2015) [1.2](8)–(9), [5.2]–[5.3], adopted in Submission 39 from the AAUS, in which it is proposed that complaints be made to the regulator for conciliation and, if successful conciliation is unlikely, referred at the complainant's request to the relevant tribunal for determination.

instance, the tribunal 'is the most appropriate forum for the resolution of substantive disputes'.<sup>13</sup>

Taking the Victorian Civil and Administrative Tribunal, Administrative Decisions Tribunal of New South Wales and Queensland Civil and Administrative Tribunal as examples, the Tribunal is an ideal forum because it is a low cost jurisdiction and is comprised of a broad range of decision makers who have experience in weighing competing interests ... (note omitted)

9.12 The OIC noted, in a different context, that this may have resource implications for QCAT.<sup>14</sup>

9.13 Respondents—including the QLS, the AAUS, QAI and the Townsville Community Legal Service Inc.—generally supported the availability of a range of remedies for a plaintiff in a civil proceeding, including:

- orders to prohibit or require certain conduct by the contravener;<sup>15</sup>
- orders for monetary compensation for loss or damage;<sup>16</sup> and
- declarations that the contravener's conduct was unlawful or that the unlawful conduct breached the plaintiff's privacy.<sup>17</sup>

9.14 Some respondents also submitted that other relief should be available, such as an apology,<sup>18</sup> an order for costs<sup>19</sup> or 'other types of relief that a court may determine to be appropriate'.<sup>20</sup> QAI submitted there should be a 'broad range of remedies that can be tailored to the circumstances of the case at hand'.

9.15 The AAUS submitted that monetary orders should be available up to a stated amount of not more than \$100 000 to compensate the complainant for loss or damage suffered, including for any injury to feelings or humiliation.<sup>21</sup> An academic

---

<sup>13</sup> AAUS and Liberty Victoria Paper (2015) [5.3], adopted in Submission 39 from the AAUS, and citing VLRC Report No 18 (2010) [7.122].

<sup>14</sup> The OIC made this observation in the context of its submission that the functions of an independent regulator under the surveillance devices legislation should not be conferred on the Information Commissioner: see [10.18]–[10.22] below.

<sup>15</sup> Eg, Submissions 13, 15, 18, 19, 22, 33, 39, 41, 43.

<sup>16</sup> Eg, Submissions 13, 15, 18, 19, 22, 33, 39, 41.

<sup>17</sup> Eg, Submissions 13, 18, 19, 22, 33, 39, 41, 43.

<sup>18</sup> Eg, Submission 19, as is provided for in relation to information privacy complaints under the *Information Privacy Act 2009* (Qld).

<sup>19</sup> Eg, Submissions 13, 22, 39.

<sup>20</sup> Eg, Submission 43.

<sup>21</sup> See AAUS and Liberty Victoria Paper (2015) [1.2](9), [5.3], adopted in Submission 39 from the AAUS. This is consistent with the provisions of the *Information Privacy Act 2009* (Qld), discussed at [9.28] below.

expressed a similar view.<sup>22</sup> Some others noted that compensation should depend on the severity of the contravention or be a matter for the court's discretion.<sup>23</sup>

9.16 Some of these respondents also submitted that non-compliance with a prohibitory or mandatory order made in civil proceedings should be treated as a criminal offence.<sup>24</sup> One member of the public submitted that 'this provides for a staged approach to enforcement of the legislation, acts as a deterrence to non-compliance and best protects privacy interests'.<sup>25</sup> The Toowoomba Regional Council agreed with this approach, 'depending on the severity' of the conduct concerned. The QCCL submitted, in contrast, that non-compliance with such an order should be dealt with as contempt.

9.17 An academic referred to a practical difficulty in giving effect to civil remedies in the context of surveillance devices, namely, where the complainant is unable to identify the operator of the device:<sup>26</sup>

In some cases the operator may be readily identified, such as where the devices are fixed on the operator's property or the device itself is labelled with the identity of the operator, as may occur with camera traps. ... Other cases, including surveillance by a camera mounted on a drone, may be more problematic. In the absence of actually witnessing and recognising the operator of the drone, such as a neighbour, the aggrieved party is likely to have no way of knowing the identity of the person who has invaded his or her privacy. It may be hoped that the Commonwealth will follow the lead of other countries such as the United States, which is proposing to implement a system of compulsory registration and real time tracking of drones. Whilst such a system might primarily be intended for safety purposes, it might also be advantageous as a means of identifying offenders not only for the purpose of prosecution for any surveillance offence that has been committed but also to enable an aggrieved person to obtain reparation.

## EXISTING PROVISIONS AND PROPOSALS

9.18 There are no specific complaints mechanisms or civil remedy provisions in the surveillance devices legislation of the other Australian states and territories.

9.19 However, proposals for reform have been made in a number of jurisdictions and guidance can be drawn from existing provisions in other legislation.<sup>27</sup> In particular, the Commission has considered relevant provisions of the IP Act, which apply in the related context of information privacy, as well as provisions in other relevant legislation, including the *Human Rights Act 2019*.

---

<sup>22</sup> Submission 19.

<sup>23</sup> Submissions 18, 22 respectively.

<sup>24</sup> Eg, Submissions 13, 18, 33, 41.

<sup>25</sup> Submission 13.

<sup>26</sup> Submission 19. As to a system of registration and tracking for drones in Australia, see [9.64] below.

<sup>27</sup> See generally, in addition to the discussion that follows in this chapter, QLRC Consultation Paper No 77 (2018) [3.265]–[3.285], [3.298]–[3.307].

## Other jurisdictions

9.20 A number of reviews in other jurisdictions have proposed the inclusion of complaints mechanisms or civil remedies in surveillance devices legislation.<sup>28</sup>

9.21 For example, the ALRC recommended that surveillance devices legislation should follow the approach taken under the *Telecommunications (Interception and Access) Act 1979* (Cth).<sup>29</sup> That Act empowers the court, where a relevant offence provision is contravened, to make ‘such orders against the defendant as [it] considers appropriate’, including an order declaring the interception or communication to have been unlawful, an order in the nature of an injunction or mandatory injunction or an order for damages.<sup>30</sup> An aggrieved person may apply to the court that convicts a person of a relevant offence, or to another court within six years after the end of the relevant interception or communication.<sup>31</sup>

9.22 The ALRC considered that this ‘would provide a quicker, cheaper and easier means of redress where an offence has occurred’ than a statutory tort or cause of action for serious invasion of privacy. It observed that:<sup>32</sup>

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.

9.23 In addition, the ALRC recommended that jurisdiction be conferred on ‘appropriate courts and tribunals’, such as civil and administrative tribunals like QCAT or specialist courts like the Queensland Planning and Environment Court,<sup>33</sup> to hear surveillance disputes between residential neighbours. It explained that:<sup>34</sup>

<sup>28</sup> See, eg, ACT Review (2016) [2.5](j), [6.47]; ALRC Report No 123 (2014) [14.85]–[14.95]; NSWLRC Interim Report No 98 (2001) [2.115]–[2.116], ch 10; VLRC Report No 18 (2010) [7.113]–[7.116]; and NZLC Report No 113 (2010) [3.105], Rec 17, discussed in QLRC Consultation Paper No 77 (2018) [3.277]–[3.284], [3.298]–[3.306].

<sup>29</sup> ALRC Report No 123 (2014) [14.85]–[14.86], Rec 14–7. The ALRC considered that federal legislation should replace the existing state and territory statutes: Rec 14–1.

<sup>30</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2–10, s 107A(6)–(7), (9)–(10). Relevantly, it is an offence under s 7(1) to intercept a communication passing over a telecommunications system; and an offence under s 63 to communicate, use or make a record of information obtained from such an interception. Part 2–10 of the Act does not limit any liability (whether criminal or civil) that a person has under any other provision of the Act or under any other law: s 107C(1).

<sup>31</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) ss 107A, 107B. 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: s 107A(2).

<sup>32</sup> ALRC Report No 123 (2014) [14.87]–[14.88].

<sup>33</sup> Ibid [14.91]–[14.92]. In Queensland, 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.

<sup>34</sup> ALRC Report No 123 (2014) Rec 14–8, [14.90], citing *Raciti v Hughes* (1995) 7 BPR 14,837, heard in the Supreme Court of New South Wales, concerning the use of sensor-activated lights and surveillance cameras aimed at the plaintiff’s backyard.



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. While such a dispute might also be settled by one neighbour seeking an injunction against the other under the law of nuisance, as in *Raciti v Hughes*, such a process involves proceedings in superior courts. It would be desirable for a lower cost forum to be made available. (note omitted)

9.24 In contrast, the NSWLRC recommended that complaints about contraventions of the surveillance devices legislation<sup>35</sup> should be made to the NSW Privacy Commissioner for conciliation and, if unable to be resolved in that way, referred to the Administrative Decisions Tribunal for decision.<sup>36</sup> The tribunal would have wide powers to grant relief, including damages of up to \$150 000, an order to prevent the continuation or repetition of the conduct, a mandatory order (for example, for the removal of surveillance devices or the destruction of surveillance material), a declaration that certain conduct is unlawful, or an order for the publication of an apology.<sup>37</sup>

9.25 The NSWLRC observed that:<sup>38</sup>

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. (note omitted)

## Other legislation in Queensland

9.26 One of the key features of the IP Act is the right of an individual to make a complaint to the Information Commissioner about a relevant entity's contravention of

<sup>35</sup> The NSWLRC recommended that the surveillance devices legislation should deal with 'overt' and 'covert' surveillance differently. Overt surveillance would be regulated by a set of legislative principles, with no criminal prohibitions but with the ability to make a complaint and seek a civil remedy, as described above. Covert surveillance would be regulated by legislative requirements for authorisation, with criminal prohibitions as well as access to the same complaint and civil remedy process as applies to overt surveillance: see NSWLRC Interim Report No 98 (2001) [10.6].

<sup>36</sup> See NSWLRC Interim Report No 98 (2001) Recs 91 to 102, 105. It also recommended that the NSW Privacy Commissioner should have power to conduct inquiries and initiate investigations into contraventions of the legislation and standing to bring (including in a representative capacity), or intervene in, tribunal proceedings.

<sup>37</sup> Ibid [10.6], Rec 112. The 'Administrative Decisions Tribunal' has since been replaced in New South Wales with the 'Civil and Administrative Tribunal'.

<sup>38</sup> 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).

the privacy principles in relation to the individual's personal information.<sup>39</sup> Primarily, a 'relevant entity' is a government agency.<sup>40</sup>

9.27 If the complaint is accepted, after making preliminary enquiries, the Information Commissioner must consider if it could be resolved through mediation and, if so, 'take all reasonable steps to cause the complaint to be mediated'.<sup>41</sup> If an agreement is reached, it may be certified by the Information Commissioner and filed by the parties with QCAT.<sup>42</sup>

9.28 If the complaint is not resolved, the complainant may request the Information Commissioner to refer the complaint to QCAT for decision.<sup>43</sup> The tribunal is to hear and decide the matter in its original jurisdiction, in accordance with the rules and procedures applying under the QCAT Act.<sup>44</sup> After hearing the complaint, the tribunal may make one or more of the following orders:<sup>45</sup>

- (a) an order that the complaint, or a part of the complaint, has been substantiated, together with, if considered appropriate, an order in accordance with 1 or more of the following—
  - (i) that an act or practice of the respondent is an interference with the privacy of the complainant for the complaint and that the respondent must not repeat or continue the act or practice;
  - (ii) that the respondent must engage in a stated reasonable act or practice to compensate for loss or damage suffered by the complainant;
  - (iii) that the respondent must apologise to the complainant for the interference with the privacy of the complainant;
  - (iv) that the respondent must make stated amendments of documents it holds;
  - (v) that the complainant is entitled to a stated amount, of not more than \$100 000, to compensate the complainant for loss or

<sup>39</sup> See *Information Privacy Act 2009* (Qld) ch 5.

<sup>40</sup> As well as a government 'agency', a 'relevant entity' includes a bound contracted service provider: *Information Privacy Act 2009* (Qld) ss 18–21, 164(2).

<sup>41</sup> *Information Privacy Act 2009* (Qld) s 171(2).

<sup>42</sup> *Information Privacy Act 2009* (Qld) ch 5 pts 1–3. Complaints may also be referred from, or to, certain other entities, including the Ombudsman, the Health Ombudsman and the Human Rights Commissioner: see ss 165(2), 169, 170.

A complaint may not be made to the Information Commissioner unless the individual has first complained to the agency directly, 45 business days have elapsed and the complainant has not received a response or they consider the response inadequate: s 166. The mediation process is confidential: *Information Privacy Act 2009* (Qld) s 153; OIC, *Privacy Complaint Handling Policy* [3.4]–[3.6] <<https://www.oic.qld.gov.au/publications/policies/privacy-complaint-handling-policy>>.

<sup>43</sup> *Information Privacy Act 2009* (Qld) ch 5 pt 4.

<sup>44</sup> *Information Privacy Act 2009* (Qld) s 198(1), (3). For example, the QCAT Act includes provisions about the tribunal's powers to make non-publication orders, direct the parties to attend a compulsory conference, direct a hearing to be held in private and deal with special witnesses: see *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pts 6, 7.

<sup>45</sup> *Information Privacy Act 2009* (Qld) s 178.

damage suffered by the complainant because of the act or practice complained of, including for any injury to the complainant's feelings or humiliation suffered by the complainant;

- (b) an order that the complaint, or a part of the complaint, has been substantiated together with an order that no further action is required to be taken;
- (c) an order that the complaint, or a part of the complaint, has not been substantiated, together with an order that the complaint or part is dismissed;
- (d) an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

9.29 Similar approaches are taken under other legislation.<sup>46</sup>

9.30 Under the *Anti-Discrimination Act 1991*, an individual who was subject to an alleged contravention of the Act may make a complaint to the Human Rights Commissioner (formerly, the Anti-Discrimination Commissioner) for conciliation or, if unresolved, referral to QCAT. The tribunal is empowered to make various orders, including orders requiring the respondent not to commit a further contravention of the Act, to do specified things to redress the loss or damage, to pay an amount of compensation the tribunal considers appropriate, or to make a private or public apology or retraction.<sup>47</sup>

9.31 The *Human Rights Act 2019* also enables an affected individual to make a complaint, to the Human Rights Commissioner, about a public entity's alleged contravention of its obligations under the Act.<sup>48</sup> If the complaint is accepted, the commissioner 'may take the reasonable action the commissioner considers appropriate to try to resolve the complaint', including discussing the complaint with the parties or conciliating the complaint.<sup>49</sup> That Act does not, however, create a civil remedy. If a complaint is not resolved, the commissioner is to give the parties a report about the complaint and the action it considers the respondent should take to ensure the compatibility of its actions with human rights.<sup>50</sup>

9.32 The complaints mechanism under the IP Act emphasises informal resolution and remedial outcomes. It 'focuses on the steps that an agency can take

<sup>46</sup> The complaints mechanism of the *Information Privacy Act 2009* (Qld) follows the general approach of the *Privacy Act 1988* (Cth). Under the federal Act, however, if a complaint is not resolved by conciliation, the Privacy Commissioner is empowered to investigate and determine the complaint, rather than referring it to a tribunal or court. The determinations that the commissioner may make are in similar terms to the orders that the tribunal may make under the IP Act: see *Privacy Act 1988* (Cth) pt V divs 1–3. Cf *EU General Data Protection Regulation* arts 77, 79, 82 which provide for data protection complaints to be made to the relevant supervisory authority, as well as a right to bring a legal action for compensation.

<sup>47</sup> See *Anti-Discrimination Act 1991* (Qld) ch 7 pt 1 divs 1, 3–4, pt 2.

<sup>48</sup> Ordinarily, a complaint is first to be made to the public entity concerned and made to the Human Rights Commissioner only if 45 business days have elapsed with no adequate response from the entity: see *Human Rights Act 2019* (Qld) s 65(1).

<sup>49</sup> *Human Rights Act 2019* (Qld) s 77(1).

<sup>50</sup> See *Human Rights Act 2019* (Qld) pt 4 div 2.

to remedy any damage arising out of the privacy breach, rather than apportioning blame' or imposing punitive measures.<sup>51</sup>

9.33 The OIC's role is not to impose a determination but to 'facilitate both parties to the complaint to find a resolution to the matter'.<sup>52</sup> Mediation 'is a collaborative process' which 'allows the parties to propose and consider a wider range of settlement options', including non-monetary outcomes. It may also 'assist in restoring or maintaining a relationship that could otherwise likely be damaged or worsened through a litigation process'.<sup>53</sup>

9.34 The steps the OIC takes in attempting to effect a settlement may include:<sup>54</sup>

- discussing the merits of the complaint with both parties;
- communicating the complainant's proposed outcomes to the agency;
- discussing any concerns that may affect movement on the proposed outcomes; and
- negotiation with both parties in terms of moving in their response to the proposed outcomes.

[The OIC] typically conduct[s] mediation by contacting both parties individually, either by telephone or in writing. In some instances [the OIC] may attempt to resolve a complaint by facilitating a meeting between the complainant and the respondent agency, either face-to-face or by teleconference.

9.35 Because the OIC is an independent agency with relevant expertise, it can provide the parties with 'authoritative information on the application of the privacy principles'.<sup>55</sup>

<sup>51</sup> OIC, *Information Sheet: What to expect when you bring a privacy complaint to OIC—a guide for complainants* (14 August 2018) 1 <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-complaints/what-to-expect-when-you-bring-a-privacy-complaint-to-oic-a-guide-for-complainants>>. See also OIC, *Guidelines—Applying the privacy principles: Privacy myths—busted!* (16 December 2015) 4 <[https://www.oic.qld.gov.au/data/assets/pdf\\_file/0017/16163/guideline-privacy-myths-busted.pdf](https://www.oic.qld.gov.au/data/assets/pdf_file/0017/16163/guideline-privacy-myths-busted.pdf)>.

<sup>52</sup> OIC, *Guidelines—Privacy principles: What to expect when OIC receives a privacy complaint—a guide for agencies* (14 August 2018) 1 <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-complaints/what-to-expect-when-oic-receives-a-privacy-complaint-a-guide-for-agencies>>.

<sup>53</sup> OIC, *Case note: How to put a price on damage suffered as a result of a privacy breach* (February 2020) <<https://www.oic.qld.gov.au/information-for/information-privacy-officers/case-notes/how-to-put-a-price-on-damage-suffered-as-a-result-of-a-privacy-breach>>. The OIC observes that mediation is also less formal and often faster than a litigation process, and that the confidential nature of mediation 'encourages frank and candid discussion'.

<sup>54</sup> OIC, above n 52, 2. Although referred to as 'mediation', the OIC's approach could also be referred to as a form of 'conciliation'. There is often considerable overlap between such processes. Typically, a conciliator may have special expertise and may take a more active, advisory role in encouraging the parties to resolve the dispute. See generally NADRAC, *Dispute Resolution Terms* (2003) 3, 5, 9.

<sup>55</sup> OIC, *Privacy Complaint Handling Policy* (2019) <<https://www.oic.qld.gov.au/publications/policies/privacy-complaint-handling-policy>> [3.9].

9.36 Where a complaint is referred to QCAT,<sup>56</sup> the tribunal may utilise its own procedures, such as compulsory conferences, to further narrow the issues in dispute and assist the parties to reach a settlement.<sup>57</sup> If a complaint proceeds to hearing and is substantiated, the tribunal may make a compensation order but is not empowered to impose penalties. To date, two information privacy complaints referred from the OIC have resulted in a compensation order, in each case for \$5000.<sup>58</sup>

## THE COMMISSION'S VIEW

9.37 In the Commission's view, this aspect of the draft Bill should have a remedial focus by providing an avenue for the resolution of complaints in a way that addresses the harm or damage caused to an individual by unlawful surveillance.

9.38 The use of surveillance devices in civil society, and the impact of surveillance on privacy, is highly contextual. The resolution of complaints in individual cases is also likely to be variable and context-dependent.

9.39 A complaints mechanism should be flexible, accessible and cost-effective for the parties. It should also be conducive to maintaining or restoring ongoing relationships between the parties. It is recognised, for example, that a likely area of complaint about the use of surveillance devices is between residential neighbours.<sup>59</sup>

9.40 The Commission also considers that, consistently with the proposals made in other jurisdictions, civil remedies should be available in appropriate circumstances. Civil remedies provide an additional safeguard for privacy by giving affected individuals an avenue for personal redress.

9.41 The legislation based on the draft Bill should operate consistently with other relevant legislation in Queensland, notably the IP Act. The IP Act has an established complaints mechanism. In common with other legislation,<sup>60</sup> it has a focus on the informal resolution of complaints through mediation by an independent regulator with specialist knowledge and expertise. It also takes a staged approach that enables unresolved complaints to be referred for hearing and determination.

9.42 There is also likely to be some interaction between the legislation based on the draft Bill and the IP Act. Where an entity who is subject to the IP Act uses a surveillance device, both the IP Act and the draft Bill may potentially apply.<sup>61</sup>

---

<sup>56</sup> Since the commencement of the *Information Privacy Act 2009* (Qld), 28 complaints have been referred by the OIC to QCAT: see the OIC's Annual Reports from 2009–10 to 2018–19 at <<https://www.oic.qld.gov.au/about/our-organisation/our-performance/annual-reports>>.

<sup>57</sup> See *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 6 div 2, including s 69.

<sup>58</sup> *PB v WorkCover Queensland Pty Ltd* [2018] QCAT 138; *RM v Queensland Police Service* [2017] QCAT 71.

<sup>59</sup> Eg, Submissions 8, 41. See also, eg, OIC, Information Sheet: Camera surveillance, video, and audio recording—a community guide (2019) 1–2; Information provided by the Dispute Resolution Branch, Department of Justice and Attorney-General (Queensland), 3 April 2019.

<sup>60</sup> See, eg, *Anti-Discrimination Act 1991* (Qld); *Human Rights Act 2019* (Qld); and *Privacy Act 1988* (Cth) at [9.29]–[9.31] above.

<sup>61</sup> Some uses of a surveillance device might also be relevant to the right to privacy in the *Human Rights Act 2019* (Qld). See also [9.51] ff and [9.83] ff below.

Although there are significant differences between them, these Acts should ideally operate in a complementary way.<sup>62</sup>

9.43 Accordingly, the Commission considers that the draft Bill should adopt an approach modelled on that of the IP Act, with appropriate modifications. The Commission recommends a three-staged approach: complaints may be made to the Surveillance Devices Commissioner (the ‘commissioner’) for mediation;<sup>63</sup> unresolved complaints may be referred to QCAT for hearing and decision; and, if appropriate, the tribunal may order remedial relief.

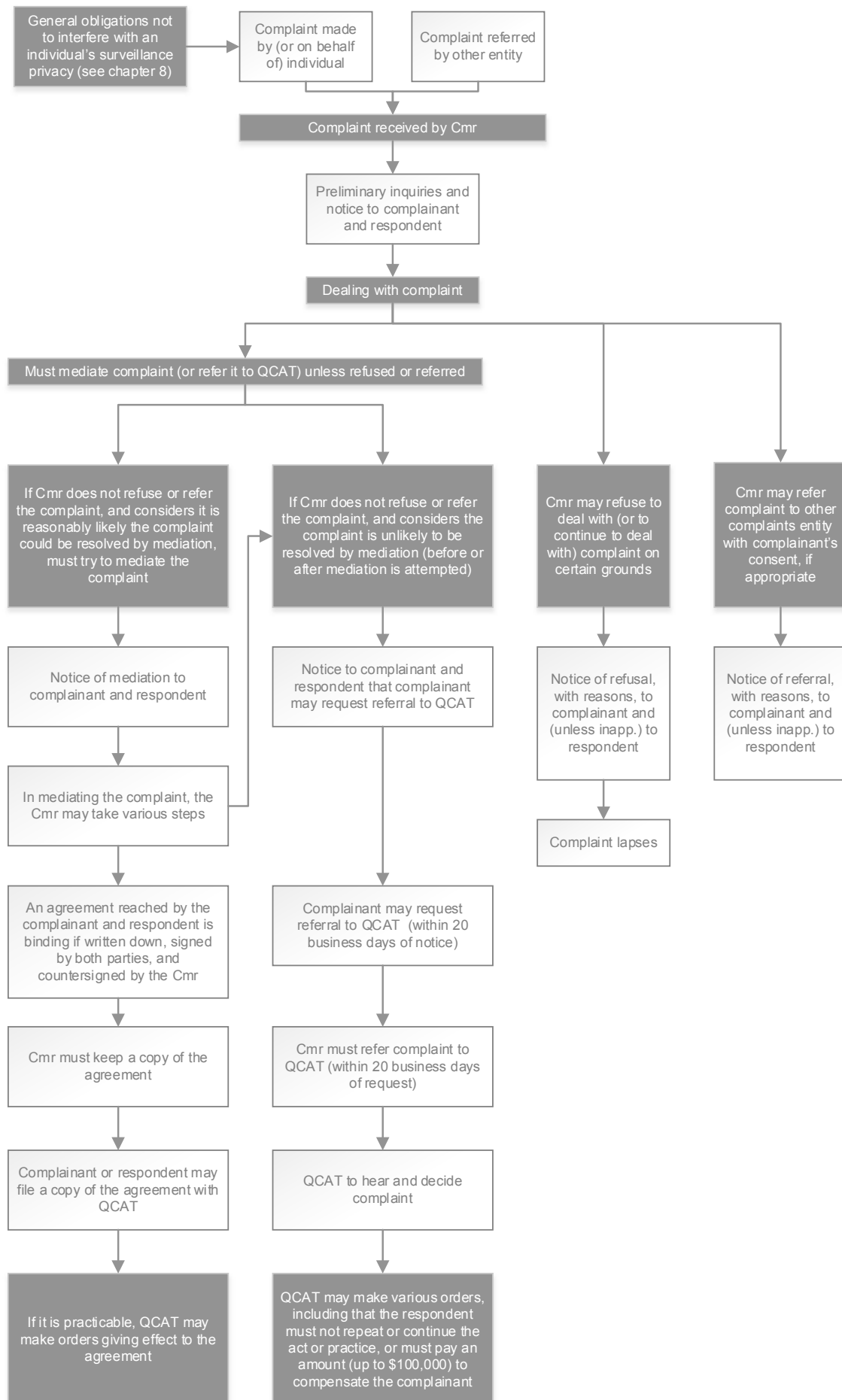
9.44 In the Commission’s view, this approach will provide a practical and meaningful protection for individual privacy in relation to the use of surveillance devices and will enhance the compatibility of the legislation with the *Human Rights Act 2019*.

9.45 The elements of the Commission’s recommended approach are outlined in the diagram on the following page and in the more detailed discussion that follows.

---

<sup>62</sup> See also Rec 4-2(a) above.

<sup>63</sup> As to the ‘Surveillance Devices Commissioner’ that the Commission recommends, see Chapter 10 below and pt 5 of the draft Bill.



## ELEMENTS OF THE RECOMMENDED APPROACH

### Making and referring complaints to the commissioner

#### *The ground for making a complaint*

9.46 In Chapter 8 above, the Commission recommends civil provisions imposing general obligations to the effect that a person must not use a surveillance device, or communicate or publish surveillance information,<sup>64</sup> in a way that interferes with an individual's surveillance privacy. The draft Bill provides that a complaint under the legislation (a 'surveillance device complaint') is a complaint about an alleged contravention of an obligation under those provisions.

9.47 A complaint may be made whether or not the conduct is being or has also been dealt with as a criminal offence.<sup>65</sup>

#### *Who may make a complaint*

9.48 The draft Bill provides that a complaint about an alleged contravention of the general obligations may be made to the commissioner by an individual who is the subject of the alleged contravention.

9.49 It also provides that a complaint may be made by an agent of the individual or by a person authorised by the commissioner, in writing, to make the complaint on the individual's behalf. This will ensure, for example, that a complaint may be made for an adult who has impaired decision-making capacity or for a child.<sup>66</sup>

9.50 Consistently with other legislation, the draft Bill also specifies that a complaint may be made jointly by two or more individuals.<sup>67</sup> This recognises that the use of a surveillance device in a given situation may affect the surveillance privacy of more than one person, such as a number of family members.

#### *Referral of a complaint from another complaints entity*

9.51 The draft Bill also provides for the referral of a complaint to the commissioner from another complaints entity.

9.52 In some situations, the use of a surveillance device may raise issues that relate to information privacy or other forms of privacy covered by different laws and complaints mechanisms. For example, the use of a drone-mounted camera could involve unlawful surveillance, the collection of personal information, or the intrusion

<sup>64</sup> Under the draft Bill, 'surveillance information' is defined to mean information obtained, directly or indirectly, using a surveillance device.

<sup>65</sup> See [8.48] above. See Chapters 5 and 6 above, which deal with the use prohibitions and the communication or publication prohibitions under the draft Bill.

<sup>66</sup> This is consistent with the *Anti-Discrimination Act 1991* (Qld) s 134(1)(b)–(c); *Human Rights Act 2019* (Qld) s 64(1)(b)–(c). Cf *Information Privacy Act 2009* (Qld) s 196 which has a similar effect.

<sup>67</sup> See *Anti-Discrimination Act 1991* (Qld) s 134(2); *Human Rights Act 2019* (Qld) s 64(3).



upon an individual's private space. In some cases, a complaint made to one entity might be better dealt with by a different complaints body.

9.53 It is necessary to ensure that, if a complaint is made to another complaints entity that would more appropriately be dealt with under the draft Bill, the complaint can be referred to the commissioner.

9.54 It is anticipated that the most likely referral entities in this context will be the Information Commissioner and the Human Rights Commissioner, which both have some privacy-related functions. However, complaints might also be made from time to time to other complaints entities, such as the Health Ombudsman, which would also appropriately be referred to the commissioner. For example, a person might complain to the Health Ombudsman about the use of visual camera surveillance in a patient examination room at a health service.

9.55 The draft Bill accordingly provides that, if any of the following entities considers that a complaint they have received may also be a complaint under the legislation, they may refer the complaint to the commissioner:<sup>68</sup>

- the Information Commissioner, in relation to a complaint received under the IP Act;
- the Human Rights Commissioner, in relation to a complaint received under the *Human Rights Act 2019*;
- the Ombudsman, in relation to a complaint received under the *Ombudsman Act 2001*;
- the Health Ombudsman, in relation to a complaint received under the *Health Ombudsman Act 2013*; or
- another entity that has received the complaint while performing its functions under a law.

9.56 Consistently with the IP Act, the provision does not require the complainant to consent to the referral of the complaint from the other entity to the commissioner under the draft Bill.<sup>69</sup> In the Commission's view, this is a matter for the legislation governing the other scheme under which the complaint was initially made.

### **Requirements for a complaint**

9.57 The draft Bill provides that a complaint made or referred to the commissioner must be made or referred within six months after the alleged contravention that is the subject of the complaint came to the complainant's

---

<sup>68</sup> In Chapter 10 below, the Commission recommends the conferral of functions and powers under the legislation on an independent regulator (the 'Surveillance Devices Commissioner'). That chapter, and the draft Bill, set out the provisions required to establish a new statutory body for this purpose. The Commission recognises in that chapter, however, that an alternative option is to confer the relevant functions and powers on an existing regulatory agency, such as the Information Commissioner within the OIC (rather than creating a new statutory body). In such a case, the referral provisions here and at [9.83]–[9.89] below may require modification to reflect that any such 'referral' would be an internal process.

<sup>69</sup> See *Information Privacy Act 2009* (Qld) s 165.

knowledge, or within a further period that the commissioner considers reasonable in the circumstances.<sup>70</sup>

9.58 This will provide a complainant with adequate time to make a complaint, whilst avoiding unnecessary delay and uncertainty for a respondent. It will also provide some flexibility and discretion to the commissioner in accepting a complaint.<sup>71</sup>

9.59 A complainant will not always be immediately aware of the use of a surveillance device, or the communication or publication of surveillance information, especially in the case of ongoing or covert surveillance. For this reason, it is preferable for the time limit to commence from the time the complainant first became aware of the alleged contravention, rather than the time when the alleged contravention first occurred.<sup>72</sup>

9.60 The draft Bill also provides that a complaint made or referred to the commissioner must be in writing, state the complainant's name and contact details (including, for example, the complainant's postal or email address), state the respondent's name, address or other contact details, if known, and include enough information to identify the alleged contravention to which the complaint relates.

9.61 Consistently with other legislation, the draft Bill requires that, for a complaint made to the commissioner by an individual, the commissioner must give reasonable help to the complainant to put the complaint in writing.<sup>73</sup> This will ensure that an individual is not prevented from making a complaint because they need assistance to put it in the required form.

9.62 The Commission recognises that, whilst the complaint should ordinarily include the respondent's name and address, an individual complainant may not always be able to identify the person who is using the surveillance device, or making the communication or publication.<sup>74</sup>

9.63 There may be situations in which the commissioner is in a better position than the complainant to identify the respondent from the particulars given in the complaint. As noted at [9.71] below, the draft Bill includes a general provision empowering the commissioner to make preliminary inquiries about the complaint. This will also empower the commissioner to request information from other entities to assist in identifying the respondent.

---

<sup>70</sup> Provision for applications to be received within a reasonable time after the prescribed period is made under the *Judicial Review Act 1991* (Qld) s 26. Cf *Information Privacy Act 2009* (Qld) s 168(1)(f) and *Human Rights Act 2019* (Qld) s 70(1)(d), which have a 12 month time limit for complaints.

<sup>71</sup> See [9.77] below. Note that decisions of the commissioner under the draft Bill will be subject to review in accordance with the provisions of the *Judicial Review Act 1991* (Qld): see Chapter 10 below.

<sup>72</sup> See, similarly, *Information Privacy Act 2009* (Qld) s 168(1)(f). Cf *Human Rights Act 2019* (Qld) s 70(1)(d).

<sup>73</sup> See *Information Privacy Act 2009* (Qld) s 166(2); *Human Rights Act 2019* (Qld) s 67(2).

<sup>74</sup> There is no express requirement in the *Information Privacy Act 2009* (Qld), *Human Rights Act 2019* (Qld) or *Anti-Discrimination Act 1991* (Qld) for the complainant to identify the respondent in the complaint. Cf *Privacy Act 1988* (Cth) s 36(5), which requires the complainant to 'specify the respondent to the complaint'.

9.64 Identification has been recognised as a particular challenge in the case of drones, which are remotely operated.<sup>75</sup> Federal drone safety regulations are continuing to develop, giving CASA an improved ability to identify drone operators. A mandatory annual registration and accreditation scheme for recreational and commercial drones is being progressively implemented from July 2019.<sup>76</sup> CASA has also begun using portable ‘drone detection surveillance equipment’ at major events and popular drone use areas to monitor drone operations and detect potential contraventions of the safety regulations.<sup>77</sup> CASA is also reportedly still developing a ‘full real-time network’ to track drones in the same way as other aircraft.<sup>78</sup>

9.65 CASA is an ‘APP entity’ for the purposes of the Privacy Act and, accordingly, may disclose personal information it collects in accordance with that Act.<sup>79</sup> Under the APPs in that Act, personal information may be disclosed in particular circumstances including, relevantly, if:<sup>80</sup>

- the use or disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order;
- the use or disclosure is reasonably necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body;
- if a ‘permitted general situation’ exists in relation to the disclosure, such as where:
  - the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or

<sup>75</sup> Eg, Submission 19 at [9.17] above. See also D Butler, ‘Drones and Invasions of Privacy: An International Comparison of Legal Responses’ (2019) 42(3) *UNSW Law Journal* 1039, 1073; J Henderson, ‘Drone law after Gatwick: legislation, registration and accreditation in Australia in 2019’ (2019) 21(10) *Internet Law Bulletin* 174; Senate Rural and Regional Affairs and Transport References Committee, Parliament of Australia, *Current 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) [4.2].

<sup>76</sup> See *Civil Aviation Safety Amendment (Remotely Piloted Aircraft and Model Aircraft—Registration and Accreditation) Regulations 2019* (Cth); CASA, ‘New rules for drone registration and accreditation’ (News), 31 July 2019; CASA, *Proposed new remotely piloted aircraft (RPA) registration and RPAS operator accreditation scheme (PP 1816US)* (31 July 2019) <<https://consultation.casa.gov.au/regulatory-program/pp1816us/>> and related documents. The requirements will apply, with some exceptions, to RPAs of more than 250g operated recreationally, and all RPAs operated commercially. This gives general effect to the recommendation in the 2018 report of the Senate Rural and Regional Affairs and Transport References Committee: see n 75 above, ch 4, Rec 2.

<sup>77</sup> CASA, ‘Drone detection action’ in *The CASA Briefing—April 2019* (16 April 2019) <<https://www.casa.gov.au/publications-and-resources/publication/casa-briefing-april-2019>>.

<sup>78</sup> J Evans, ‘Drone “flyer’s licence” to be launched in time for Google’s world-first delivery service in Canberra’, *ABC News* (online), 27 March 2019.

<sup>79</sup> See generally CASA, *Civil Aviation Safety Authority privacy policy* (9 July 2019) <<https://www.casa.gov.au/privacy-policy>>. CASA is also authorised to disclose information under the *Civil Aviation Safety Regulations 1998* (Cth) s 201.016 in particular circumstances where it ‘necessary for the safety of air navigation’. Uncommenced amendments to those regulations by the *Civil Aviation Safety Amendment (Remotely Piloted Aircraft and Model Aircraft—Registration and Accreditation) Regulations 2019* (Cth) ss 22–24 will additionally provide for CASA to disclose information to an enforcement body for enforcement related activities.

<sup>80</sup> *Privacy Act 1988* (Cth) ss 14, 16A(1) table items 4, 5; sch 1 APP 6, 6.2(b)–(c), (e).

- the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

9.66 The Commission recommends that the Queensland Government should take steps to facilitate a memorandum of understanding between CASA and the commissioner about the sharing of information by CASA about registered owners and accredited flyers of drones for the purpose of complaints under the draft Bill.

9.67 Unlike the IP Act and the *Human Rights Act 2019*, the draft Bill does not require the complainant to first make a formal complaint to the respondent and await a minimum time before submitting the complaint to the commissioner.<sup>81</sup> Given that the draft Bill applies not just to government agencies but also to organisations and individuals, such a requirement would in many cases be impractical and could unnecessarily complicate or delay the handling of the complaint.<sup>82</sup>

### Dealing with complaints

9.68 The draft Bill sets out the way the commissioner is to deal with a complaint made or referred to it, including by refusing to deal with the complaint, referring the complaint to another complaints entity, or attempting to resolve the complaint by mediation.<sup>83</sup>

### Preliminary notice and inquiries

9.69 As soon as practicable after receiving a complaint, the commissioner must give a notice to the complainant and respondent stating the substance of the complaint, the commissioner's role in dealing with the complaint and that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint. The notice to the respondent must also require the respondent to advise the commissioner of the respondent's contact details (including, for example, the respondent's postal or email address).

9.70 This will ensure that both parties receive the same statement of the complaint and of the commissioner's role in dealing with the complaint after it has been received.<sup>84</sup>

9.71 The draft Bill empowers the commissioner to make preliminary inquiries about the complaint to decide how to deal with the complaint under this part of the legislation. This will enable the commissioner to obtain additional information that is

---

<sup>81</sup> See *Information Privacy Act 2009* (Qld) s 166(3) and *Human Rights Act 2019* (Qld) s 65, at nn 42, 48 above. Those Acts apply to government agencies and public entities.

<sup>82</sup> It has been observed that the requirement in the *Information Privacy Act 2009* (Qld) s 166(3) can be overly onerous, frustrating and potentially inefficient, and that the OIC should be given greater discretion and flexibility to accept complaints earlier or later than the 45 business day timeframe: see PricewaterhouseCoopers, 'Strategic Review of the Office of the Information Commissioner' (Report, 26 April 2017) [3.2.1], Rec (c); and Department of Justice and Attorney-General (Queensland), 'Review of the *Right to Information Act 2009* and *Information Privacy Act 2009*' (Report, October 2017) 41–2, Rec 17.

<sup>83</sup> There should be a clear administrative division between the commissioner's complaints handling, mediation and other functions: see [10.108] below.

<sup>84</sup> Depending on the circumstances, this notice might be given at the same time as the further notice required to be given, at [9.79], [9.87], or [9.93] below, once the commissioner decides how to deal with the complaint.

necessary to decide if the commissioner is authorised to deal with the complaint, and whether the commissioner may refuse to deal with the complaint or refer it to another entity. The provision will also empower the commissioner to make inquiries, if necessary, to identify the respondent to the complaint.<sup>85</sup>

9.72 This is not limited to inquiries made of the complainant or respondent, but would also allow the commissioner to make inquiries of another entity that has possession or control of information relevant to the complaint, such as a referring entity that has referred the complaint to the commissioner.<sup>86</sup>

9.73 In Chapter 10 below, the Commission recommends specific provision to empower the commissioner to give notice to a person (including the complainant or respondent) asking or directing them to provide relevant information or a document within the reasonable period stated in the notice. This provision will apply for the purpose of making preliminary inquiries about a complaint (as well as for the mediation of a complaint, or the performance of the commissioner's other functions under the legislation).<sup>87</sup>

### ***Direction to protect privacy of complainant or respondent***

9.74 The draft Bill also includes a general provision, consistently with other legislation,<sup>88</sup> to empower the commissioner to give a notice directing a person not to communicate or publish information that identifies, or is likely to identify, the complainant or respondent to the complaint. The commissioner may give such a direction if satisfied on reasonable grounds that it is necessary to protect the privacy of the complainant or respondent. For the reasons outlined at [10.145] below, non-compliance with a direction is an offence with a maximum penalty of 10 penalty units. This does not apply, however, if there is a reasonable excuse (for example, where the complainant or respondent is seeking legal advice in relation to the complaint).

### ***Refusing to deal with a complaint***

9.75 The commissioner may decide that a complaint should not proceed.

9.76 If a matter does not constitute a 'complaint' within the meaning of the draft Bill, it will fall outside the commissioner's jurisdiction and can be declined administratively. This will apply if the matter does not relate to an alleged contravention of an obligation at [9.46] above.<sup>89</sup>

9.77 If a matter is a 'complaint' within the meaning of the draft Bill, there may still be reasons why it should not proceed. The draft Bill provides that the commissioner

---

<sup>85</sup> See [9.62]–[9.66] above.

<sup>86</sup> A similar approach is taken in the *Human Rights Act 2019* (Qld) s 68. Cf *Information Privacy Act 2009* (Qld) s 167, which is limited to inquiries of the complainant or respondent.

<sup>87</sup> See Rec 10-8(c) below. See also [9.94] and [10.105] below. Failure to comply with a direction in such a notice, without a reasonable excuse, is an offence with a maximum penalty of 10 penalty units: Rec 10-18(e)(ii) below.

<sup>88</sup> See *Human Rights Act 2019* (Qld) s 100.

<sup>89</sup> See, in particular, the definitions of 'complaint' and 'surveillance device complaint' in the draft Bill cl 39(1) and sch 1.

may refuse to deal with a complaint, or part of a complaint, made or referred to the commissioner if:<sup>90</sup>

- the commissioner considers that:
  - the complaint or part does not comply with the requirements in [9.60] above about the matters that must be stated in the complaint;
  - there is a more appropriate course of action available under another law to deal with the subject of the complaint or part; or
  - the subject of the complaint or part has been appropriately dealt with by another entity;
- the complaint or part was not made or referred to the commissioner within the time required at [9.57] above; or
- the complaint or part is frivolous, trivial, vexatious, misconceived or lacking in substance.

9.78 The draft Bill also provides that the commissioner may refuse to continue dealing with a complaint, or part of a complaint, under any of the above grounds or if:<sup>91</sup>

- the complainant does not comply with a reasonable request made by the commissioner in dealing with the complaint or part;
- the commissioner is satisfied on reasonable grounds that the complainant, without a reasonable excuse, has not cooperated in the commissioner's dealing with the complaint or part;
- the commissioner cannot make contact with the complainant (for example, because the complainant has not given current contact details).

9.79 If the commissioner refuses to deal with the complaint, or to continue to deal with the complaint, the commissioner must give the complainant notice of the refusal, with reasons. The commissioner must also give notice of the refusal, with reasons, to the respondent, unless the commissioner considers it is not necessary to do so. (This might apply, for example, if the respondent is not yet aware of, or has not been contacted by the commissioner about, the complaint).<sup>92</sup>

9.80 To avoid doubt, the draft Bill provides that, if the complaint is refused, the complaint lapses (and a new complaint about the same alleged contravention cannot be made by the same complainant).

<sup>90</sup> Cf *Information Privacy Act 2009* (Qld) s 168(1)(a)–(d), (f). See also *Human Rights Act 2019* (Qld) ss 69, 70(1)(a)–(c); *Anti-Discrimination Act 1991* (Qld) ss 139, 140(2).

<sup>91</sup> Cf *Human Rights Act 2019* (Qld) s 70(1), (2)(a)–(c); *Information Privacy Act 2009* (Qld) s 168(2)(a)–(c).

<sup>92</sup> Similar provision is made in the *Human Rights Act 2019* (Qld) s 71(2).

9.81 The provisions for refusal (or referral)<sup>93</sup> of a complaint will ensure that the commissioner is able to deal with complaints in an appropriate and efficient way. They will also ensure that the commissioner retains discretion in the individual circumstances whether to deal with a complaint, rather than automatically restricting the complaints that may accepted.

9.82 If the commissioner considers it is necessary to delay dealing with a complaint in order to ensure, for example, that the complaint can be dealt with under another law, general principles of administrative law and natural justice will operate.

### ***Referral of complaints to other entities***

9.83 The draft Bill also empowers the commissioner to refer a complaint that it has received to another relevant complaints entity.

9.84 This recognises that a complaint may be made to the commissioner under the draft Bill which might more appropriately be dealt with by a different entity. It complements the provision for complaints to be referred to the commissioner under the draft Bill from other entities.<sup>94</sup> These provisions will assist in providing a more streamlined process for complainants by removing the need for them to submit a new complaint to a different entity.

9.85 The draft Bill provides that, if the subject of the complaint could be the subject of a privacy complaint under the IP Act, the commissioner may refer the complaint to the Information Commissioner.<sup>95</sup> It similarly provides for the referral of a relevant complaint to the Human Rights Commissioner, the Ombudsman or the Health Ombudsman.

9.86 Consistently with other legislation, the draft Bill also provides that the commissioner may refer a complaint to one of those entities only with the complainant's consent and if the commissioner considers the complaint would be more appropriately dealt with by the entity to whom it is referred.<sup>96</sup> This will ensure that a complaint is not unnecessarily delayed, or dealt with inadequately, by an inappropriate referral. Given that different outcomes or remedies may be available under different complaints schemes, the Commission considers that the complainant's consent to the referral should be required in this context.<sup>97</sup>

9.87 The draft Bill further provides that, if a complaint is referred to another entity under this provision, the commissioner may, with the consent of the complainant, give the entity information about the complaint obtained by the commissioner, and must give the complainant notice of the referral, with reasons. The commissioner must also give notice of the referral, with reasons, to the respondent, unless the commissioner considers it is not necessary to do so (for example, if the respondent

---

93 See [9.83] ff below.

94 See [9.55] above.

95 But see n 68 above.

96 See *Human Rights Act 2019* (Qld) s 73(6).

97 In particular, there is no standalone civil remedy under the *Human Rights Act 2019* (Qld) and, if a complaint is not resolved by the Human Rights Commissioner under that Act there is no provision for the complaint to be referred to a tribunal or court for hearing and decision: see [9.31] above.

is not yet aware of, or has not been contacted by the commissioner about, the complaint).

### **Arrangements with other entities**

9.88 To assist in dealing with and managing the referral of complaints to, or from, the Information Commissioner, the Human Rights Commissioner, the Ombudsman or the Health Ombudsman, the draft Bill provides for the commissioner to enter into, and act in accordance with, arrangements with any of those entities (a 'referral entity').<sup>98</sup> Consistently with other legislation, an arrangement may provide for:<sup>99</sup>

- the types of complaint under the draft Bill that the commissioner should refer to the referral entity (and how the referral is made);
- the types of complaint made to a referral entity that should be referred to the commissioner (and how the referral is made);
- dealing with a complaint or other matter under a referral entity's legislation that could also form the basis of a complaint under the draft Bill; or
- cooperating in the performance by the commissioner and the referral entity in their respective functions to ensure the effective operation of the draft Bill and the referral entity's legislation.

9.89 This will ensure that any referrals between the commissioner and those entities are managed in an efficient and effective way, having regard to their respective functions and roles.

## **Mediation of complaints**

### **Attempting resolution by mediation**

9.90 If the commissioner does not refuse the complaint or refer it to another entity, reasonable steps are to be taken to attempt to resolve the complaint through mediation.<sup>100</sup> This stage of the Commission's recommended approach focuses on the parties reaching their own resolution to the complaint.

9.91 The draft Bill provides that the purpose of mediation is to identify and clarify the issues in the complaint and to promote the resolution of the complaint in a way that is informal, quick and efficient.<sup>101</sup>

<sup>98</sup> The draft Bill includes definitions, that are relevant for this provision, of 'referral Act' and 'referral entity'.

<sup>99</sup> See *Information Privacy Act 2009* (Qld) s 170; *Human Rights Act 2019* (Qld) s 74.

Such an arrangement would also need to take into account relevant legislative requirements, including the requirement, at [9.86] above, for the complainant to consent to a referral made by the commissioner to the Information Commissioner or Human Rights Commissioner. See also n 68 above.

<sup>100</sup> Consistently with the *Information Privacy Act 2009* (Qld), the term 'mediation' is used here. Other Acts, such as the *Human Rights Act 2019* (Qld), use the term 'conciliation'. These are not necessarily precise terms and there is often some overlap between them: see generally NADRAC, *Dispute Resolution Terms* (2003) 3, 5, 9.

<sup>101</sup> See NADRAC, *Dispute Resolution Terms* (2003) 9 (definition of 'mediation'). See also, eg, *Human Rights Act 2019* (Qld) s 80; *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ss 77, 66C, 66D(a)(i), 69(a).



9.92 It provides that the commissioner must try to mediate the complaint if:<sup>102</sup>

- in the commissioner's opinion, it is reasonably likely that the complaint could be resolved by mediation; and
- the commissioner does not refuse the complaint or refer it to another entity, under the provisions at [9.77]–[9.79] and [9.83]–[9.87] above.

9.93 Where this applies, the commissioner is required to give notice of the mediation to the complainant and respondent, stating the substance of the complaint, the powers that the commissioner may exercise in trying to resolve the complaint by mediation, and that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint. The notice to the respondent must also state that the respondent will have an opportunity to respond to the complaint in writing.<sup>103</sup>

9.94 The draft Bill provides that the commissioner may take the reasonable action it considers appropriate to try to resolve the complaint by mediation. Without limiting this, the commissioner is empowered to:<sup>104</sup>

- ask the respondent to respond in writing to the complaint;
- give the complainant a copy of the respondent's written response;
- ask or direct the complainant or respondent to give the commissioner information (or documents) relevant to the complaint, including by notice;<sup>105</sup>
- make enquiries of, and discuss the complaint with, the complainant and respondent;
- provide information to the complainant and respondent about the legislation and how it applies to the complaint;
- facilitate a meeting between the complainant and respondent.

9.95 The commissioner may, in accordance with the provision the Commission recommends in Chapter 10 below, delegate the commissioner's functions and powers relating to the mediation of complaints to an appropriately qualified member of the commission's staff.<sup>106</sup>

9.96 The provisions above will provide a flexible approach and ensure that the complaints mechanism is accessible and responsive to the parties' individual circumstances. The steps above could be undertaken in person or on the papers. In

---

<sup>102</sup> See, similarly, *Information Privacy Act 2009* (Qld) s 171.

<sup>103</sup> Cf *Human Rights Act 2019* (Qld) s 76(2)–(3).

<sup>104</sup> These steps are also generally consistent with the approach taken by the OIC in mediating an information privacy complaint under the IP Act: see [9.34] above. See also, eg, *Human Rights Act 2019* (Qld) s 77(2); *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 66D.

<sup>105</sup> See [9.69]–[9.73] above and [10.105] below. Under the draft Bill, 'information' is defined to include a record in any form and a document.

<sup>106</sup> See Rec 10-6 below.

some circumstances, it might be appropriate for the parties to attend a face-to-face 'conference' with the commissioner. However, in many cases this will not be practical and negotiations between the parties can be facilitated in other ways.<sup>107</sup>

9.97 In mediating a complaint, the commissioner would provide information about the legislation to assist the parties to reach a resolution, but would not make any binding legal determinations.<sup>108</sup>

### **Confidentiality of mediation**

9.98 To encourage open discussion and good faith negotiation, the draft Bill also ensures the confidentiality of the mediation. It provides that a person who is or has been the commissioner or a member of staff of the commission must not disclose information coming to their knowledge during a mediation. However, this does not apply if the disclosure is made:

- with the consent of the complainant and respondent;
- for the purpose of giving effect to the commissioner's complaints handling or reporting functions under the legislation;
- for statistical purposes without identifying a person to whom the information relates;
- for an inquiry or proceeding about an offence happening during the mediation;
- for a proceeding founded on fraud alleged to be connected with, or to have happened during, the mediation; or
- under a requirement imposed by an Act.

9.99 Consistently with other legislation, the draft Bill further provides that evidence of anything said or done, or an admission made, in the course of the mediation of a complaint is admissible in a civil proceeding only if the complainant and respondent agree. This does not apply, however, to a civil proceeding founded on fraud alleged to be connected with, or to have happened, during the mediation. Neither is this provision intended to prevent the complainant or respondent from filing a copy of the signed written agreement reached at mediation, with QCAT, in accordance with the provisions at [9.102] below.

9.100 These provisions are consistent with the approach taken to the confidentiality of 'ADR processes' under the *Civil Proceedings Act 2011*.<sup>109</sup>

<sup>107</sup> See, eg, the steps used by the OIC for complaints under the *Information Privacy Act 2009* (Qld) at [9.34] above.

<sup>108</sup> This is consistent with the approach taken by the OIC in its guidelines about the *Information Privacy Act 2009* (Qld): see generally OIC, *Guidelines* (2019) <<https://www.oic.qld.gov.au/guidelines>>. See also, in relation to the commissioner's guidance functions, [10.109] below.

<sup>109</sup> See *Civil Proceedings Act 2011* (Qld) ss 53, 54. Provisions in similar terms are also included in other legislation, such as the *Magistrates Courts Act 1921* (Qld) ss 42O, 42Q.

### ***Mediated agreement***

9.101 The draft Bill provides that, if the complainant and respondent agree to a resolution of the complaint at the mediation, the agreement is not binding (as a 'mediated agreement') until it is written down, signed by the complainant and respondent and certified by the commissioner as the agreement signed by the parties in accordance with the provision.<sup>110</sup> The commissioner must also keep a copy of the mediated agreement.

9.102 The draft Bill further provides that either the complainant or respondent may file a copy of the mediated agreement with QCAT and that the tribunal may, in certain circumstances, make orders necessary to give effect to the agreement.<sup>111</sup> The tribunal may make an order only if it is satisfied that:<sup>112</sup>

- the order is consistent with an order the tribunal may make under the provision at [9.123] below or under the QCAT Act; and
- it is practicable to implement the order.

9.103 An order made by the tribunal under this provision is, and may be enforced as, an order of the tribunal under the QCAT Act.<sup>113</sup>

9.104 These provisions will ensure that, where appropriate, an agreement reached at mediation will have a binding effect. This approach is generally consistent with the way in which agreements reached during mediation are treated under the *Civil Proceedings Act 2011*.<sup>114</sup>

### **Referral of complaints to tribunal**

9.105 Most complaints are likely to be resolved by mediation. However, a mediated outcome agreed to by the parties may not always be achievable. In those cases, the complaint should be referred to QCAT for hearing and decision.<sup>115</sup> This will ensure that, where necessary, a binding determination can be made and enforced.

9.106 In the Commission's view, QCAT is the preferred forum in this context. The tribunal has jurisdiction for a range of specialist civil and administrative matters, including matters under the IP Act and the *Anti-Discrimination Act 1991*, and is the

---

<sup>110</sup> 'Sign' includes the attaching of a seal and the making of a mark: *Acts Interpretation Act 1954* (Qld) s 36 sch 1 (definition of 'sign').

<sup>111</sup> If there is a concern that the agreement filed with QCAT is not a true copy, the tribunal could exercise its general power under s 63 of the *Queensland Civil and Administrative Tribunal Act 2009* (Qld) to require the commissioner to produce the copy of the agreement the commissioner is required to keep under the provision at [9.101] above.

<sup>112</sup> This is generally consistent with the *Information Privacy Act 2009* (Qld) s 173.

<sup>113</sup> See [9.128] ff below.

<sup>114</sup> See *Civil Proceedings Act 2011* (Qld) ss 48, 50. See also s 49(1); and *Uniform Civil Procedure Rules 1999* (Qld) r 331, Form 35 (Mediator's certificate).

<sup>115</sup> Under the similar model that operates under the *Information Privacy Act 2009* (Qld), only a small number of complaints are referred by the OIC to QCAT: see [9.36], n 56 above.

best available to incorporate new jurisdictions, assuming adequate resourcing.<sup>116</sup> It has an established jurisdiction in dealing with information privacy complaints under the IP Act and it is constituted by members with specialist experience and expertise.<sup>117</sup> The tribunal's procedures are flexible and it is required to deal with matters in a way that is 'accessible, fair, just, economical, informal and quick'.<sup>118</sup> The tribunal may conduct proceedings by remote conferencing or on the papers, in appropriate cases.<sup>119</sup> The tribunal's practices and procedures focus on assisting and dealing with self-represented parties and on pre-hearing procedures to expedite and promote the settlement of matters. Referral of unresolved complaints to QCAT is also consistent with the approach taken under the IP Act.

9.107 The Commission recommends that QCAT be provided with any additional resources that are necessary to ensure the effective operation of the proposed new jurisdiction conferred on it by the draft Bill.

### ***When a complaint is referred***

9.108 This aspect of the draft Bill applies if:

- the commissioner does not refuse to deal with the complaint or refer it to another entity, under the provisions at [9.77]–[9.79] and [9.83]–[9.87] above; and
- in the commissioner's opinion, the complaint is unlikely to be resolved:
  - by mediation of the complaint; or
  - despite attempts to mediate the complaint.

9.109 In those circumstances, the commissioner must give notice to the complainant and respondent that these provisions apply and that the commissioner will, if asked by the complainant to do so, refer the complaint to QCAT to decide.

9.110 The draft Bill provides that the complainant may give the commissioner a written request for referral of the complaint to QCAT, within 20 business days after receiving the commissioner's notice. A time limit on the complainant's request will

<sup>116</sup> QCAT is specifically intended to 'provide a streamlined framework' for civil and administrative disputes, and was designed to 'be able to incorporate new and emerging jurisdictions in the future': Queensland, *Parliamentary Debates*, Legislative Assembly, 19 May 2009, 351 (CR Dick, Attorney-General and Minister for Industrial Relations). See also Explanatory Notes, Queensland Civil and Administrative Tribunal Bill 2009 (Qld) 3–4.

<sup>117</sup> As to the constitution of the tribunal, see [9.122] below.

<sup>118</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 3(b). See also s 4 which provides that, to achieve the objects of the Act, the tribunal must, among other things, encourage the early and economical resolution of disputes before the tribunal including, if appropriate, through alternative dispute resolution processes; ensure proceedings are conducted in an informal way that minimises costs to parties and is as quick as is consistent with achieving justice; ensure the tribunal is accessible and responsive to the diverse needs of persons who use the tribunal; and maintain and ensure the appropriate use of the specialist knowledge, expertise and experience of members and adjudicators.

<sup>119</sup> See *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 32.

provide some certainty for respondents and ensure that complaints can be finalised in a timely way.<sup>120</sup>

9.111 Where such a request is made by the complainant, the draft Bill requires the commissioner to refer the complaint to QCAT within 20 business days after the request.<sup>121</sup>

9.112 These provisions are generally consistent with the approach under the IP Act.<sup>122</sup>

### ***Tribunal's jurisdiction and procedure***

9.113 The draft Bill provides that, where the complaint is referred by the commissioner to QCAT, the tribunal must exercise its original jurisdiction under the QCAT Act to hear and decide the complaint.<sup>123</sup> The complainant and respondent to the complaint are both parties to the QCAT proceeding; the complainant is taken to be the applicant for the proceeding; and the respondent to the complaint is taken to be the respondent for the proceeding.

9.114 The rules and procedures applying to the tribunal under the QCAT Act apply, including provisions about notice<sup>124</sup> and fees.<sup>125</sup> This will enable matters about the conduct of proceedings to be considered on a case-by-case basis, having regard to the particular circumstances.<sup>126</sup>

9.115 For example, in appropriate cases, the tribunal may use its power under that Act to conduct a compulsory conference with the parties to further narrow the issues in dispute and promote a settlement. In some limited circumstances, the tribunal might also consider it appropriate to refer the matter to further mediation or

<sup>120</sup> Cf *Anti-Discrimination Act 1991* (Qld) s 166 which provides, in general, a time limit of 28 days (but with an ability for the commissioner to extend the time limit). In contrast, under the *Information Privacy Act 2009* (Qld) pt 4 there is no time limit on the complainant's request for referral.

<sup>121</sup> Under *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 34(2)(a), a referral of a matter to the tribunal under an enabling Act 'must be made within the period provided for under the enabling Act'.

<sup>122</sup> See *Information Privacy Act 2009* (Qld) ss 174, 175, 176(1). Cf *Anti-Discrimination Act 1991* (Qld) ss 164A, 165–166.

<sup>123</sup> See *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ss 9, 10(1)(b), 15(b) as to the tribunal's original jurisdiction. See also s 16 of that Act which provides that, '[i]n exercising its original jurisdiction conferred by an enabling Act, the tribunal may perform the functions conferred on the tribunal by this Act or the enabling Act'. As to the form in which a referral must be made, see s 34 of that Act and *Queensland Civil and Administrative Tribunal Rules 2009* (Qld) rr 9, 10.

<sup>124</sup> Notice of a proceeding started by a referral must be given by the applicant to each of the parties (but is not required to be given to the referring entity): *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 37(1)–(2); *Queensland Civil and Administrative Tribunal Rules 2009* (Qld) r 22.

<sup>125</sup> Ordinarily, the fee for a referral made to QCAT is \$345.80, but no fee is payable if the referral is made by a 'State-related person': *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 38(1); *Queensland Civil and Administrative Tribunal Regulation 2009* (Qld) s 8(2). In instances where the Information Commissioner refers a complaint to QCAT under the IP Act, there is no fee payable: Information provided by QCAT, 20 February 2020.

<sup>126</sup> Subject to the requirements of the QCAT Act and the enabling Act, the procedure of the tribunal is in the tribunal's discretion: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 28(1).

conciliation.<sup>127</sup> This would continue the focus under this part of the draft Bill on informal dispute resolution.

9.116 The tribunal also has power, if necessary, to direct that a hearing or part of a hearing be held in private, or to make a non-publication order about information in a proceeding.<sup>128</sup> Although proceedings should ordinarily be open, this would enable additional steps to be taken to protect the complainant's, or another individual's, privacy in exceptional cases.

9.117 The QCAT Act also empowers the tribunal to direct that two or more proceedings concerning the same or related facts and circumstances be consolidated into one proceeding, or remain as separate proceedings but be heard and decided together.<sup>129</sup> As noted earlier, it is possible in some circumstances that the subject matter of a complaint made under the draft Bill could also relate to the subject matter of a separate complaint under the IP Act.<sup>130</sup> In such a case, where the complaints are both referred to QCAT, it may be highly desirable for the tribunal to hear and decide the complaints together.

9.118 It is also noted that, under the *Human Rights Act 2019*, a human rights claim under that Act may be added to another existing cause of action under other legislation.<sup>131</sup> This may enable a complainant under the draft Bill to add a human rights claim to the complaint before the tribunal.

9.119 The provision at [9.113] above will also ensure that the other provisions of general application under the QCAT Act will operate, including provisions about appeals from tribunal decisions.<sup>132</sup>

<sup>127</sup> See *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 6 divs 1A, 2, 3.

<sup>128</sup> The tribunal may direct a hearing or part of a hearing to be held in private, or may make a non-publication order, if it considers it is necessary to: (a) avoid interfering with the proper administration of justice; (b) to avoid endangering the physical or mental health or safety of a person; (c) to avoid offending public decency or morality; (d) to avoid the publication of confidential information or information whose publication would be contrary to the public interest; or (e) for any other reason in the interests of justice: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ss 66(2), 90(2). A non-publication order may prohibit the publication (except in the way and to the persons stated in the order) of the contents of a document produced to the tribunal, evidence given before the tribunal, or information that may enable a person who has appeared before the tribunal, or is affected by a proceeding, to be identified: s 66(1).

See also s 125(2) which provides that, if the tribunal publishes its final decision or reasons, it must ensure it does not include something the subject of a non-publication order. This may result, for example, in the de-identification of a party.

<sup>129</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 5 div 4, ss 54(1), 55(1)(a). The tribunal may also direct that the proceedings be heard in a particular sequence: s 55(1)(b).

<sup>130</sup> See generally [9.42] above.

<sup>131</sup> *Human Rights Act 2019* (Qld) s 59. There is no standalone cause of action under the *Human Rights Act 2019* (Qld). However, if a person may seek any relief or remedy in relation to an act or decision of a public entity on the ground that the act or decision was, other than under the *Human Rights Act 2019* (Qld) s 58, unlawful, the person may add the ground of unlawfulness under the *Human Rights Act 2019* (Qld) to the other claim, and may obtain the same relief (except monetary damages) that could have been obtained under the other claim, even if that other claim does not also succeed.

<sup>132</sup> A party may appeal against a tribunal decision to the Appeal Tribunal of QCAT (if the decision was made by a non-judicial member) or to the Court of Appeal (if the decision was made by a judicial member). A decision of the Appeal Tribunal may be appealed on a question of law to the Court of Appeal: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 8.

9.120 However, the draft Bill modifies the provisions of the QCAT Act in relation to the constitution of the tribunal.<sup>133</sup>

9.121 Ordinarily under the QCAT Act, the president is to choose one or more members or an adjudicator to constitute the tribunal for a particular matter.<sup>134</sup> In addition to the president and deputy president, the QCAT Act relevantly provides for the appointment of senior members, ordinary members, supplementary members and adjudicators. The QCAT Act also confers certain functions and powers on judicial members and legally qualified members. Each class of member has a different level of experience or qualification.<sup>135</sup>

9.122 The draft Bill provides that, for a hearing conducted by the tribunal in relation to a complaint referred to it under the legislation, the tribunal is to be constituted by at least one member who is a legally qualified member.<sup>136</sup> This will retain the president's discretion in how the tribunal is constituted, but will ensure that a complaint under the draft Bill is heard by at least one member who is an Australian lawyer of at least six years standing or is a magistrate or a judicial member.<sup>137</sup> It will also ensure that the tribunal as constituted for hearing a complaint may, if appropriate, exercise the power to consolidate two or more proceedings or to grant an injunction or interim injunction.<sup>138</sup>

### **Orders the tribunal may make**

9.123 The draft Bill provides that, after the hearing of a complaint referred to QCAT, the tribunal may make one or more of the following final decisions:

- an order that declares the respondent's use, communication or publication contravened a general obligation at [8.44] above in relation to the complainant and, if the tribunal considers appropriate, includes one or more of the following—

<sup>133</sup> An enabling Act that confers original jurisdiction on the tribunal may 'add to, otherwise vary, or exclude' functions of the QCAT or provisions of the QCAT Act about various matters: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 6(2)(a), (3), (7)–(8). A modifying provision in an enabling Act prevails over the provisions of the QCAT Act to the extent of any inconsistency: s 7(1)–(2). One of the matters that an enabling Act may provide for is the way in which the tribunal is to be constituted for a particular matter: s 167(4).

<sup>134</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 165(1). In doing so, the president is to consider: the nature, importance and complexity of the matter; the need for the tribunal hearing the matter to have special knowledge, expertise or experience relating to the matter; any provision of the QCAT Act, enabling Act or the rules that may be relevant; and any other matter the president considers relevant: s 167(1).

<sup>135</sup> For example, a senior member must be an Australian lawyer of at least eight years standing, or a person having extensive knowledge, expertise or experience relating to a relevant class of matter; an ordinary member must be an Australian lawyer of at least six years standing, or a person having special knowledge, expertise or experience relating to a relevant class of matter; and a supplementary member must be a Supreme Court judge, District Court judge or a magistrate. See generally *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 4 pts 3, 4, ss 171(2), 183, 192, sch 3 Dictionary.

<sup>136</sup> This is generally consistent with the *Anti-Discrimination Act 1991* (Qld) s 176.

<sup>137</sup> A 'legally qualified member' is a judicial member; an ordinary member or supplementary member who is a magistrate; or a senior member or ordinary member who is an Australian lawyer of at least six years standing: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 8 sch 3 Dictionary (definition of 'legally qualified member'). A 'judicial member' is the president; the deputy president; or a supplementary member who is a Supreme Court judge or District Court judge: s 8 sch 3 Dictionary (definition of 'judicial member').

<sup>138</sup> Those powers are exercisable only by a legally qualified member: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ss 54(2), 59(4).

- (a) an order that the respondent must not repeat or continue a stated act or practice;
- (b) an order that the respondent must compensate the complainant for loss or damage (including for injury to the complainant's feelings or humiliation) suffered because of the respondent's act or practice by:
  - (i) engaging in a stated act or practice; or
  - (ii) paying the complainant a stated amount of not more than \$100 000;
- an order dismissing the complaint, or part of the complaint;
- an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

9.124 This is consistent with the orders the tribunal may make after hearing an information privacy complaint under the IP Act, or an anti-discrimination complaint under the *Anti-Discrimination Act 1991*. It is also generally consistent with the types of orders that may be made by a court under the *Telecommunications (Interception and Access) Act 1979* (Cth) and with the recommendations of the ALRC and NSWLRC.<sup>139</sup>

9.125 It is important to provide a broad range of possible remedies to enable redress of any harm caused by the respondent's contravention. As well as an order requiring the respondent to stop certain conduct, it is desirable to allow for an order that the respondent take specific steps to redress the complainant's loss or damage, for example, by removing or changing the location of a CCTV camera<sup>140</sup> or, in an appropriate circumstance, giving an apology or making a retraction. The OIC notes that, in its experience, non-financial outcomes such as an apology are often sought by privacy complainants.<sup>141</sup> Along with a declaration that the respondent has contravened the legislation, an apology may provide acknowledgment of the wrong and assist in redressing the damage suffered by the complainant.

9.126 In cases where the contravention has resulted in particularly significant and serious harm, it is appropriate that monetary compensation be available as a possible outcome. Consistently with the IP Act, however, the amount that may be awarded should be capped at \$100 000. The aim of an order made under this part of the draft Bill should be remedial, rather than punitive.

<sup>139</sup> See [9.21], [9.24], [9.28], [9.30] above. It is also consistent with the types of determinations that may be made by the Information Commissioner under the *Privacy Act 1988* (Cth): see [9.29] n 46 above.

<sup>140</sup> See, eg, Information and Privacy Commission NSW, 'Attitudes of the NSW Community to Privacy 2017' (Report, 2017), Attachment [4.5] in which 37% of respondents considered that an order requiring a neighbour to remove privacy-invasive cameras would be a preferred outcome.

<sup>141</sup> OIC, *Case note: How to put a price on damage suffered as a result of a privacy breach* (May 2018); OIC, *News: The art of the apology* (9 February 2016) <<https://www.oic.qld.gov.au/about/news/the-art-of-the-apology>>. An apology does not constitute an admission of fault or liability and is not relevant to the determination of fault or liability in relation to the matter: *Civil Liability Act 2003* (Qld) s 72D.



9.127 Under the QCAT Act, the tribunal has a general power when making a decision to impose conditions on the decision.<sup>142</sup> In the Commission's view, it is important to ensure that the terms of the order are clear. Accordingly, the draft Bill provides that an order made by the tribunal under the provisions at [9.123](b) above, which require the respondent to take a specified action, must state the reasonable time within which the relevant action must be taken.

### Enforcement of tribunal orders

9.128 Under the QCAT Act, a final decision of the tribunal is binding on all the parties.<sup>143</sup>

9.129 A QCAT decision may be enforced by accessing the enforcement procedures of the courts.<sup>144</sup>

9.130 A party to the decision may file a certified copy of the decision, along with an affidavit about the other party's non-compliance with the decision, in the registry of a court of competent jurisdiction. Relevantly in the present context, this will be a Magistrates Court (for a monetary decision of up to \$100 000)<sup>145</sup> or the Supreme Court (for a non-monetary decision).<sup>146</sup> On filing, the tribunal's decision is taken to be an order of the court in which it is filed and may be enforced accordingly.<sup>147</sup>

9.131 The procedures for enforcement differ depending on the nature of the order. Enforcement of a monetary order usually involves an application for an 'enforcement warrant or order', for example, to authorise the sale of property, redirection of earnings, or payment of instalments in satisfaction of the monetary order.<sup>148</sup> Enforcement of a non-monetary order, where the respondent has not complied with a requirement in the order to perform or abstain from an act, is enforceable by punishment for contempt (such as by a fine or imprisonment),<sup>149</sup> or by an enforcement warrant authorising the seizure and detention of property.<sup>150</sup>

<sup>142</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 114(a).

<sup>143</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 126(1).

<sup>144</sup> See *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ch 2 pt 7 div 4; *Uniform Civil Procedure Rules 1999* (Qld) chs 19–20.

<sup>145</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 131(2); *Magistrates Courts Act 1921* (Qld) ss 2 (definition of 'prescribed limit'), 4.

<sup>146</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 132(2). The Supreme Court may, however, transfer the enforcement proceeding to a Magistrates Court or the District Court if the order is of a kind that may be made by, or is otherwise capable of being enforced in that court: *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 132(4)–(6).

<sup>147</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) ss 131(3), 132(3).

<sup>148</sup> See *Uniform Civil Procedure Rules 1999* (Qld) ch 19. In particular, see ch 19 pts 4–10, especially rr 828, 855, 868.

<sup>149</sup> If the respondent is an individual, the court may punish the individual for contempt by making an order that may be made under the *Penalties and Sentences Act 1992* (Qld); if the respondent is a corporation, the court may punish the respondent by seizing corporation property or imposing a fine or both. See *Uniform Civil Procedure Rules 1999* (Qld) r 930(2), (3).

<sup>150</sup> See *Uniform Civil Procedure Rules 1999* (Qld) ch 20. In particular, see ch 20 pt 2 rr 898, 904, 917–920 and pt 7 rr 925(1)(a), 930.

9.132 The QCAT Act also contains an offence provision for non-compliance with QCAT orders. It is an offence—punishable by a fine of up to \$13 345—for a person to contravene a non-monetary decision of the tribunal, without reasonable excuse.<sup>151</sup>

9.133 Non-compliance with a non-monetary order made by QCAT may also constitute contempt of the tribunal and be punished accordingly.<sup>152</sup> A person may not, however, be punished twice for the same conduct.<sup>153</sup>

9.134 In the Commission's view, the enforcement of QCAT decisions is adequately provided for under the provisions of general application under the QCAT Act. The availability of the enforcement procedures of the courts, including the ability in relevant cases to deal with non-compliance as a contempt, provides appropriate enforcement options for tribunal orders made under the legislation. Further, the existing offence provision under the QCAT Act for the contravention of a non-monetary decision will enable non-compliance with an order made under the legislation to be dealt with as a criminal matter in appropriate cases.

9.135 Accordingly, it is not necessary for the draft Bill to include an additional, specific offence for non-compliance with a tribunal order made under the legislation.

## RECOMMENDATIONS

### **A complaints mechanism**

**9-1 The draft Bill should provide a mechanism for complaints about alleged contraventions of the general obligations in Recommendation 8-2 above ('surveillance device complaints') to the effect that:**

- (a) complaints may be made to the Surveillance Devices Commissioner (the 'commissioner') established under Recommendation 10-2(b) below for mediation;**
- (b) complaints not resolved by mediation may be referred to QCAT for hearing and decision; and**

<sup>151</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 213. The maximum penalty for this offence is 100 penalty units (\$13 345). The prescribed value of a penalty unit is \$133.45: *Penalties and Sentences Act 1992* (Qld) ss 5(1)(e)(i), 5A; *Penalties and Sentences Regulation 2015* (Qld) s 3.

<sup>152</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 218. QCAT has the same powers and jurisdiction as the Supreme Court in relation to contempt, and the provisions dealing with contempt under the *Uniform Civil Procedure Rules 1999* (Qld) apply: s 219(1)–(2). However, 'QCAT does not recommend the use of contempt proceedings as a first step in enforcing QCAT decisions' as the enforcement procedures of the courts 'may be faster and more cost-effective': QCAT, *Application for contempt, including non-compliance with decisions* (16 September 2016) <<https://www.qcat.qld.gov.au/qcat-decisions/contempt/contempt-applications>>.

<sup>153</sup> *Queensland Civil and Administrative Tribunal Act 2009* (Qld) s 221. In particular, if a person's conduct is both contempt of the tribunal and an offence, the person may be proceeded against for the contempt or the offence, but is not liable to be punished twice for the same conduct: s 221(2).

(c) if appropriate, the tribunal may order remedial relief.

The complaints mechanism should have the features set out below.

*[See Surveillance Devices Bill 2020 pt 4, cl 39 and [9.37]–[9.45] above]*

**Making and referring complaints to the commissioner**

**9-2 A complaint under Recommendation 9-1 above:**

(a) may be made to the commissioner:

- (i) by an individual who is the subject of the alleged contravention;
- (ii) by an agent of the individual; or
- (iii) by a person authorised by the commissioner in writing to make the complaint for the individual; and

(b) may be made under paragraph (a) jointly by or for two or more individuals.

*[See Surveillance Devices Bill 2020 cl 40, and [9.48]–[9.50] above.]*

**9-3 A complaint may be referred to the commissioner by any of the following entities, if they consider that the complaint may also be a complaint under this legislation:**

- (a) the Information Commissioner, in relation to a complaint received under the *Information Privacy Act 2009*;
- (b) the Human Rights Commissioner, in relation to a complaint received under the *Human Rights Act 2019*;
- (c) the Ombudsman, in relation to a complaint received under the *Ombudsman Act 2001*;
- (d) the Health Ombudsman, in relation to a complaint received under the *Health Ombudsman Act 2013*; or
- (e) any other entity that has received the complaint in performing its functions under a law [including a law of another State or the Commonwealth].

*[See Surveillance Devices Bill 2020 cl 41, sch 1 (definitions of ‘referral Act’ and ‘referral entity’), and [9.51]–[9.56] above.]*

- 9-4** A complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above must be in writing, state the complainant's name and contact details (including, for example, the complainant's postal or email address), state the respondent's name, address or other contact details if they are known, and include enough information to identify the alleged contravention to which the complaint relates.

*[See Surveillance Devices Bill 2020 cl 42(1), and [9.60] above.]*

- 9-5** A complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above must be made or referred within six months after the alleged contravention that is the subject of the complaint came to the complainant's knowledge, or within a further period that the commissioner considers is reasonable in all the circumstances.

*[See Surveillance Devices Bill 2020 cl 43, and [9.57]–[9.59] above.]*

- 9-6** For a complaint made to the commissioner by an individual under Recommendation 9-2 above, the commissioner must give reasonable help to the complainant to put the complaint in writing.

*[See Surveillance Devices Bill 2020 cl 42(2), and [9.61] above.]*

#### **Dealing with complaints**

- 9-7** The draft Bill should set out the way in which the commissioner is to deal with a complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above.

*[See Surveillance Devices Bill 2020 cl 44, and [9.68] above.]*

#### **Preliminary notice and inquiries**

- 9-8** As soon as practicable after receiving a complaint made or referred to the commissioner under Recommendation 9-2 or 9-3 above, the commissioner must give a notice to the complainant and respondent stating:

- (a) the substance of the complaint;
- (b) the role of the commissioner in dealing with the complaint; and
- (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint.

The notice to the respondent must also require the respondent to advise the commissioner of the respondent's contact details, including, for example, the respondent's postal or email address.

*[See Surveillance Devices Bill 2020 cl 46, and [9.69]–[9.70] above.]*

- 9-9** Where a complaint is made or referred to the commissioner under Recommendation 9-2 or 9-3 above, the commissioner may make preliminary inquiries about the complaint to decide how to deal with the complaint and, if the complaint does not include enough information to do so, to identify the respondent to the complaint.

*[See Surveillance Devices Bill 2020 cl 45, and [9.71]–[9.72] above.]*

- 9-10** The Queensland Government should take steps to facilitate a memorandum of understanding between CASA and the commissioner about the sharing of information by CASA about registered owners and accredited flyers of drones for the purpose of complaints under the legislation.

*[See [9.64]–[9.66] above.]*

**Direction to protect privacy of complainant or respondent**

- 9-11** In dealing with a complaint, the commissioner may, by notice, direct a person not to communicate or publish information that identifies, or is likely to identify, the complainant or respondent to a complaint if the commissioner is satisfied on reasonable grounds that it is necessary to do so to protect the privacy of the complainant or respondent. Non-compliance with a direction, without reasonable excuse, should be an offence with a maximum penalty of 10 penalty units.

*[See Surveillance Devices Bill 2020 cl 47, and [9.74] above.]*

**Refusing to deal with a complaint**

- 9-12** The commissioner may refuse to deal with a complaint, or part of a complaint, if:

- (a) the commissioner considers that:
- (i) the complaint does not comply with the requirements at Recommendation 9-4 above about the matters that must be stated in the complaint;
  - (ii) there is a more appropriate course of action available under another law to deal with the subject of the complaint or part;
  - (iii) the subject of the complaint or part has been appropriately dealt with by another entity; or

- (b) the complaint or part was not made or referred to the commissioner within the time stated at Recommendation 9-5 above; or
- (c) the complaint or part is frivolous, trivial, vexatious, misconceived or lacking in substance;

*[See Surveillance Devices Bill 2020 cll 17, 48(1), and [9.77] above.]*

**9-13** The commissioner may refuse to continue to deal with a complaint, or part of a complaint, under any of the grounds in Recommendation 9-12 above or if:

- (a) the complainant does not comply with a reasonable request made by the commissioner in dealing with the complaint or part;
- (b) the commissioner is satisfied on reasonable grounds that the complainant, without a reasonable excuse, has not cooperated in the commissioner's dealing with the complaint or part; or
- (c) the commissioner can not make contact with the complainant.

*[See Surveillance Devices Bill 2020 cll 17, 48(2), and [9.78] above.]*

**9-14** If the commissioner refuses to deal with a complaint or to continue dealing with a complaint under Recommendation 9-12 or 9-13 above:

- (a) the commissioner must give notice of the refusal, with reasons, to the complainant and, unless the commissioner considers it is not necessary to do so in the circumstances, to the respondent; and
- (b) the complaint lapses, and the complainant cannot make a further complaint under this legislation about the same alleged contravention.

*[See Surveillance Devices Bill 2020 cll 49 and 50, and [9.79]–[9.80] above.]*

#### **Referral of complaints to other entities**

**9-15** The commissioner may refer a complaint to another entity as follows, if it considers the complaint would be more appropriately dealt with by the other entity and if the complainant consents:

- (a) if the subject of the complaint could be the subject of a privacy complaint under the *Information Privacy Act 2009*, the commissioner may refer the complaint to the Information Commissioner;

- (b) if the subject of the complaint could be the subject of a human rights complaint under the *Human Rights Act 2019*, the commissioner may refer the complaint to the Human Rights Commissioner;
- (c) if the subject of the complaint could be the subject of a complaint under the *Ombudsman Act 2001*, the commissioner may refer the complaint to the Ombudsman;
- (d) if the subject of the complaint could be the subject of a health service complaint under the *Health Ombudsman Act 2013*, the commissioner may refer the complaint to the Health Ombudsman.

*[See Surveillance Devices Bill 2020 cl 51(1)–(2), and [9.83]–[9.85] above.]*

**9-16** If the commissioner refers a complaint under Recommendation 9-15 above to another entity, the commissioner:

- (a) may, with the complainant's consent, give the entity information about the complaint obtained by the commissioner; and
- (b) must give notice of the referral, with reasons, to the complainant and, unless the commissioner considers it is not necessary to do so in the circumstances, to the respondent.

*[See Surveillance Devices Bill 2020 cl 51(3)–(4), and [9.86]–[9.87] above.]*

#### **Arrangements with other entities**

**9-17** The commissioner may enter into an arrangement with the Information Commissioner, the Human Rights Commissioner, the Ombudsman or the Health Ombudsman (a 'referral entity') to provide for:

- (a) the types of complaint under the legislation that the commissioner should refer to the referral entity (under Recommendation 9-15 above), and how the referral is made;
- (b) the types of complaint made under a referral Act that the referral entity should refer to the commissioner (under Recommendation 9-3 above), and how the referral is made;
- (c) dealing with a complaint or other matter under a referral Act that could also form the basis of a complaint under the legislation; or
- (d) cooperating in the performance by the commissioner and the referral entity in their respective functions to ensure the effective operation of the legislation and the referral entity's legislation.

*[See Surveillance Devices Bill 2020 cl 52, sch 1 (definitions of 'referral Act' and 'referral entity'), and [9.88]–[9.89] above.]*

**Mediation of complaints**

- 9-18** The draft Bill should specify that the purpose of mediation is to identify and clarify the issues in the complaint and to promote the resolution of the complaint in a way that is informal, quick and efficient.

*[See Surveillance Devices Bill 2020 cl 53, and [9.91] above.]*

- 9-19** The commissioner must try to mediate the complaint if:

- (a) in the commissioner's opinion, it is reasonably likely the complaint could be resolved by mediation; and
- (b) the commissioner does not:
  - (i) refuse to deal with, or to continue to deal with, the complaint, under Recommendation 9-12 or 9-13 above; or
  - (ii) refer the complaint to another entity under Recommendation 9-15 above.

*[See Surveillance Devices Bill 2020 cl 54(1), and [9.90], [9.92] above.]*

- 9-20** Where Recommendation 9-19 applies, the commissioner must give notice of the mediation to the complainant and respondent stating:

- (a) the substance of the complaint;
- (b) the powers the commissioner may exercise in trying to resolve the complaint by mediation; and
- (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint.

The notice to the respondent must also state that the respondent will have an opportunity to respond to the complaint in writing.

*[See Surveillance Devices Bill 2020 cl 55, and [9.93] above.]*

- 9-21** The commissioner may take the reasonable action the commissioner considers appropriate to try to resolve the complaint by mediation. Without limiting the steps the commissioner may take, the commissioner may:

- (a) ask the respondent to respond in writing to the complaint;
- (b) give the complainant a copy of the respondent's written response;



- (c) ask or direct the complainant or respondent to give the commissioner information relevant to the complaint, including by notice given under Recommendation 10-8(c) below;
- (d) make enquiries of, and discuss the complaint with, the complainant and respondent;
- (e) provide information to the complainant and respondent about the legislation and how it applies to the complaint; or
- (f) facilitate a meeting between the complainant and respondent.

*[See Surveillance Devices Bill 2020 cl 54(2)–(3), sch 1 (definition of ‘information’), and [9.94]–[9.97] above.]*

#### **Confidentiality of mediation**

**9-22** A person who is or has been the commissioner or a staff member of the commission must not disclose information coming to their knowledge during a mediation. However, this does not apply if the disclosure is made:

- (a) with the consent of the complainant and respondent to the complaint;
- (b) for the purpose of giving effect to the commissioner’s complaints handling or reporting functions under the legislation;
- (c) for statistical purposes without identifying a person to whom the information relates;
- (d) for an inquiry or proceeding about an offence happening during the mediation;
- (e) for a proceeding founded on fraud alleged to be connected with, or to have happened during, the mediation; or
- (f) under a requirement imposed by an Act.

*[See Surveillance Devices Bill 2020 cl 56, and [9.98] above.]*

**9-23** Evidence of anything said or done, or an admission made, in the course of the mediation of a complaint is admissible in a civil proceeding only if the complainant and respondent agree. However:

- (a) This provision does not apply to a mediated agreement filed with QCAT under Recommendation 9-25 below; and

- (b) A ‘civil proceeding’ for this provision does not include a civil proceeding founded on fraud alleged to be connected with, or to have happened, during the mediation.

*[See Surveillance Devices Bill 2020 cl 57, and [9.99] above.]*

#### **Mediated agreement**

- 9-24** If, after mediation, the complainant and respondent agree to resolve the complaint:

- (a) the agreement is not binding, as a ‘mediated agreement’, until it is written down, signed by the complainant and respondent and certified by the commissioner as the agreement signed by the parties in accordance with these requirements;

- (b) the commissioner must keep a copy of the mediated agreement.

*[See Surveillance Devices Bill 2020 cl 58, and [9.101] above.]*

- 9-25** The complainant or respondent may file a copy of the mediated agreement prepared under Recommendation 9-24 above with QCAT.

*[See Surveillance Devices Bill 2020 cl 59(1), and [9.102] above.]*

- 9-26** If a mediated agreement is filed with QCAT under Recommendation 9-25 above, the tribunal may make orders necessary to give effect to the agreement if the tribunal is satisfied that:

- (a) the order is consistent with an order the tribunal may make under Recommendation 9-31 below or the QCAT Act; and

- (b) it is practicable to implement the order.

An order made by the tribunal under this provision is, and may be enforced as, an order of the tribunal under the QCAT Act.

*[See Surveillance Devices Bill 2020 cl 59(2)–(3), and [9.102]–[9.103] above.]*

#### **Referral of complaints to tribunal**

- 9-27** The draft Bill should provide that, if:

- (a) the commissioner does not:

- (i) refuse to deal with, or to continue to deal with, the complaint, under Recommendation 9-12 or 9-13 above; or

- (ii) refer the complaint to another entity under Recommendation 9-15 above; and

(b) in the commissioner's opinion, the complaint is unlikely to be resolved:

(i) by mediation of the complaint; or

(ii) despite attempts to mediate the complaint

the commissioner must give notice to the complainant and respondent that these provisions apply and that the commissioner will, if asked to do so by the complainant, refer the complaint to QCAT to decide.

*[See Surveillance Devices Bill 2020 cll 60 and 61, and [9.108]–[9.109] above.]*

**9-28** The complainant may, in writing to the commissioner, ask for the referral of the complaint to QCAT within 20 business days after receiving notice under Recommendation 9-27 above.

*[See Surveillance Devices Bill 2020 cl 62(1), and [9.110] above.]*

**9-29** The commissioner must refer the complaint to QCAT within 20 business days after receiving a request made under Recommendation 9-28 above.

*[See Surveillance Devices Bill 2020 cl 62(2), and [9.111] above.]*

#### **Tribunal's jurisdiction and procedure**

**9-30** Where a complaint is referred to QCAT under Recommendation 9-29 above:

(a) the tribunal must exercise its original jurisdiction under the QCAT Act to hear and decide the complaint;

(b) the complainant and respondent to the complaint are both parties to the proceeding;

(c) the complainant is taken to be the applicant for the proceeding;

(d) the respondent is taken to be the respondent for the proceeding;

(e) subject to para (f) below, the rules and procedures applying to QCAT under the QCAT Act apply to the proceeding; and

(f) for a hearing conducted by the tribunal in relation to the complaint, the tribunal is to be constituted by at least one legally qualified member.

*[See Surveillance Devices Bill 2020 cll 62(3), 63 and 64, and [9.113]–[9.122] above.]*

**9-31** After the hearing of a complaint referred to QCAT under Recommendation 9-29 above, the tribunal may make one or more of the following final decisions to decide the complaint:

- (a) an order that declares the respondent's use, communication or publication contravened a general obligation in Recommendation 8-2(a) or (b) above in relation to the complainant and, if QCAT considers appropriate, includes one or more of the following—
  - (i) an order that the respondent must not repeat or continue a stated act or practice;
  - (ii) an order that the respondent must compensate the complainant for loss or damage (including for injury to the complainant's feelings or humiliation) suffered because of the respondent's act or practice by:
    - (A) engaging in a stated act or practice; or
    - (B) paying the complainant a stated amount of not more than \$100 000;
- (b) an order dismissing the complaint, or part of the complaint;
- (c) an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

*[See Surveillance Devices Bill 2020 cl 17, 65(1)–(2), and [9.123]–[9.126] above.]*

**9-32** An order made by the tribunal under Recommendation 9-31(a)(ii) above must state the reasonable time within which the relevant action must be taken.

*[See Surveillance Devices Bill 2020 cl 65(3), and [9.127] above.]*

### **Resourcing**

**9-33** QCAT should be provided with any additional resources necessary to ensure the effective operation of the new jurisdiction conferred on the tribunal by the legislation.

*[See [9.107] above.]*

# Chapter 10

## A new regulator

INTRODUCTION .....	271
SUBMISSIONS.....	271
An independent regulator .....	271
The regulator's functions and powers .....	276
EXISTING PROVISIONS AND PROPOSALS .....	278
Other jurisdictions .....	279
Other legislation in Queensland .....	283
THE COMMISSION'S VIEW .....	287
Which entity .....	287
ELEMENTS OF THE RECOMMENDED APPROACH .....	291
Establishment of the regulator .....	291
Functions and powers .....	293
Reporting requirements.....	299
Protections and offences.....	301
Review of decisions .....	303
RECOMMENDATIONS .....	303

### INTRODUCTION

10.1 The terms of reference require the Commission to consider appropriate regulatory powers and enforcement mechanisms, and to otherwise appropriately protect the privacy of individuals in relation to the use of surveillance devices. The terms of reference also direct the Commission to consider 'whether any particular authority is best placed' to exercise any required regulatory or enforcement powers.<sup>1</sup>

10.2 In the Consultation Paper, the Commission sought submissions on whether there should be an independent regulator and, if so, what entity this should be and what regulatory and compliance functions or powers it should have.<sup>2</sup>

### SUBMISSIONS

#### An independent regulator

10.3 The majority of respondents who addressed these questions—including QGCIO, the Department of Education, Future Wise, the AAUS, the Brisbane City Council, the QLS, QAI, the OIC and several members of the public—agreed that the

---

<sup>1</sup> See terms of reference, paras 4, 6 and D in Appendix A.

<sup>2</sup> See QLRC Consultation Paper No 77 (2018) Q-28 and Q-29.

surveillance devices legislation should confer oversight functions on an independent regulator.<sup>3</sup>

10.4 The OIC expressed in-principle support for an independent regulator to ensure that the use of surveillance devices is ‘transparent and accountable and subject to rigorous governance and oversight mechanisms’. It also observed that:

The creation of independent regulators to respond to particular challenges posed by emerging technology is not without precedent in other jurisdictions. For example, the UK office of the Surveillance Camera Commissioner was created under the *Protection of Freedoms Act 2012* to further regulate CCTV. The Biometrics Commissioner was also established by the *Protection of Freedoms Act 2012* to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints.<sup>4</sup> (notes omitted; note added)

10.5 The Department of Environment and Science submitted that the conferral of functions on an independent oversight body would be beneficial in supporting best practice:

The department also sees benefit in a regulatory scheme that would aim to support best practices in industry or agency dealings with members of the community through for example, developing best practice guidelines and providing advice to ensure compliance. ... [It would also] ensure that an independent agency is monitoring the growing potential of surveillance, and regularly bringing issues concerning surveillance to attention.

10.6 An academic similarly submitted that there is a need for an independent regulator in providing guidance and education about the use of surveillance devices by government agencies and others:<sup>5</sup>

For example, those engaged in occupations that may use surveillance devices as part of their normal operations, such as journalists, licensed private investigators, loss adjusters and licensed security providers may benefit from best practice guides for the use of such devices. Further, surveillance devices in the form of cameras mounted on drones have become more affordable and widely available through their sale by electronic and department stores. This has meant that surveillance devices are now in the hands of many who may have no understanding or appreciation of the laws concerning surveillance and/or the consequences for those whose privacy may be breached by imprudent use of those devices. There would be a pressing need for education of these operators as well.

10.7 A member of the public submitted that:<sup>6</sup>

Police will usually be ... unable to deal with most of these types of issues, yet individuals require a source to turn to in difficult circumstances.

---

<sup>3</sup> Submissions 10, 12, 13, 16, 19, 22, 25, 29, 32, 33, 35, 38, 39, 40, 41, 43.

<sup>4</sup> As to the position in England and Wales, see the discussion at [10.39]–[10.44] below.

<sup>5</sup> Submission 19.

<sup>6</sup> Submission 22.

10.8 Another member of the public submitted that an independent regulator would enhance the enforcement of the legislation:<sup>7</sup>

Based on my experiences there is a very clear contradiction and disconnect between the legislative and enforcement arm ... regarding the *Invasion of Privacy Act*. The legislative arm tells us one thing and [the] enforcement arm tells us something else ...

Because of this disconnect between Government departments and agencies, there needs to be [an] independent body, like an Ombudsman, appointed so complaints about legislation and enforcement can be fully and independently investigated ... Staff in the Ombudsman's office would need to be highly trained and experienced in digital technologies and the Internet of Things (IoT).

10.9 Other respondents noted the need for any new regulator to be adequately resourced and to have a wide range of relevant regulatory and technological knowledge and expertise.<sup>8</sup> QAI emphasised the need for the regulator to be 'aware and informed of issues that impact upon the surveillance of certain people, including people with disability and mental illness'.

10.10 The Department of Agriculture and Fisheries did not express a view, noting that 'this is a decision for government as it will require additional resourcing'.

### **Which entity**

10.11 Submissions were fairly evenly divided as to whether the surveillance devices legislation should confer the functions of an independent regulator on a new entity established for that purpose, or on an existing entity.

10.12 Some respondents—including the QLS, Future Wise and the Brisbane City Council—supported the establishment of a new regulatory body,<sup>9</sup> such as an 'Ombudsman'<sup>10</sup> or a 'Surveillance and Technology Adjudicator/Commissioner'.<sup>11</sup>

10.13 Other respondents—including the AAUS and QGCIO—submitted that the functions of the regulator should be conferred on the OIC or the Privacy Commissioner.<sup>12</sup> A few respondents alternatively submitted that the functions should be conferred on, or shared with, the QHRC.<sup>13</sup>

10.14 QGCIO submitted that, of the existing entities, the OIC would be best placed to take on this role:

---

<sup>7</sup> Submission 12.

<sup>8</sup> Eg, Submissions 13, 38.

<sup>9</sup> Eg, Submissions 12, 13, 22, 25, 35, 43.

<sup>10</sup> Submissions 12, 13, 25.

<sup>11</sup> Submission 22.

<sup>12</sup> Eg, Submissions 10, 19, 29, 32, 35, 39. As explained at [10.54]–[10.59] below, the OIC comprises the Information Commissioner and OIC staff. The Privacy Commissioner's role under the IP Act is that of a deputy to the Information Commissioner.

<sup>13</sup> Eg, Submissions 13, 40, 41.

QGCIO considers that any enforcement or regulatory powers enabled by the new legislative framework should exist within an independent statutory authority that administers information and data legislation more broadly. As acknowledged by the consultation paper, it is difficult to identify a suitable statutory authority with the appropriate existing remit to administer the new legislative framework due to the complexity and applicability of existing legislation. Whilst acknowledging the limitations of its current remit, QGCIO suggests that the Office of the Information Commissioner Queensland would be the statutory authority that is best placed to administer any new legislative framework. As the consultation paper highlights, there exists some close alignment with the existing role that OIC plays in:

- providing best practice guidance and advice about legislation that it currently administers
- research, leadership and reporting on matters relevant to its legislation
- administration of complaints and the issuance of compliance notices

10.15 QGCIO also observed that the OIC might, in the future, take on a wider privacy role:

Considering the emergent need for broader information and data reform in Queensland, one might also consider that the OIC may play a stronger role in data and privacy reform into the future—that which may extend to beyond its current remit.

10.16 The idea of a wider or more general privacy agency was echoed in some other submissions. For example, a member of the public submitted that the Privacy Commissioner should be separated from the OIC and given responsibility to ‘administer a new complaints process to deal with alleged breaches of the privacy either by surveillance technologies or other means’.<sup>14</sup> An academic submitted that:<sup>15</sup>

Permanent oversight of the right to privacy in Queensland should be allocated to a specialised government agency. This agency should be able to collect information on breaches of privacy, resolve complaints from members of the public, and recommend new legislative or other protections.

10.17 The AAUS submitted that ‘it is more appropriate to extend the functions of existing privacy or personal information regulators than to create a new regulator’, stating that this would be ‘more cost-effective and should minimise the burden on government agencies and organisations’.<sup>16</sup>

10.18 However, the OIC did not consider that any existing entity, including the OIC, is well placed to take on this role:

The question as to which entity should be the independent regulator is complex and requires careful consideration. A review of existing entities and their

<sup>14</sup> Submission 29. An academic suggested, in contrast, that the Information Commissioner be ‘redesignated as the “Privacy Commissioner” and given new responsibilities under the surveillance devices legislation: Submission 19.

<sup>15</sup> Submission 17.

<sup>16</sup> AAUS and Liberty Victoria Paper (2015) [5], adopted in Submission 39 from the AAUS, and citing VLRC Report No 18 (2010) [5.99].



functions fails to identify any one entity that represents a natural fit with the functions and powers required to independently regulate surveillance devices legislation in Queensland—noting this will depend on the type and breadth of functions to be performed by an independent regulator. For example:

- The regulatory and compliance mechanism of the *Invasion of Privacy Act 1971* is 'primarily criminal, relying on police investigation and prosecution of offences'.<sup>17</sup> ...
- OIC's jurisdiction is limited to protecting people's personal information held by Queensland government entities and does not extend to individuals, the private sector or bodily or other types of privacy. ...
- The proposed jurisdiction of the Human Rights Commission under the Queensland Human Rights Bill 2018, while establishing statutory protection for the right to privacy, is limited to entities performing public sector functions and forms part of the suite of other administrative law obligations and oversight mechanisms that aim to hold the government accountable.<sup>18</sup> (notes omitted; notes added)

10.19 The OIC acknowledged suggestions and recommendations in other jurisdictions for functions under surveillance devices legislation to be conferred on existing information privacy regulators, but observed that, to date, those recommendations have not been implemented.<sup>19</sup> It noted that the OIC 'forms part of the integrity and accountability framework in Queensland' and expressed concern that:

The surveillance devices regulatory framework under consideration in this review would represent a significant expansion, and change in nature, of OIC's current jurisdiction.

10.20 In particular, the OIC submitted that the role of an independent regulator under the surveillance devices legislation would involve both quantitatively and qualitatively different stakeholders and issues:

As outlined above, we currently regulate about 230 Queensland larger government agencies, with other very small entities such as boards usually supported by larger agencies. Surveillance legislation may cover individuals and small businesses that are not currently regulated by the Australian or Queensland privacy legislation.<sup>20</sup> In Queensland there are 4 703 193 individuals<sup>21</sup> and more than 426 000 small businesses.<sup>22</sup> Smartphones, tablets, CCTV, body worn

<sup>17</sup> Citing QLRC Consultation Paper No 77 (2018) [3.286].

<sup>18</sup> Citing Explanatory Notes, Human Rights Bill 2018 (Qld) 6.

<sup>19</sup> The NSW Privacy Commissioner's submission, whilst not expressing a view on this issue, also observed that recommendations made in that jurisdiction for the expansion of its role in relation to surveillance devices and serious invasions of privacy have not been implemented: see the NSWLRC Interim Report No 98 (2001), discussed at [10.46]–[10.47] below, and NSW Parliamentary Committee Report (2016).

<sup>20</sup> That is, the *Information Privacy Act 2009* (Qld) or the *Privacy Act 1988* (Cth).

<sup>21</sup> Citing Australian Bureau of Statistics, *2016 Census QuickStats* (23 October 2017) <[https://quickstats.censusdata.abs.gov.au/census\\_services/getproduct/census/2016/quickstat/3?opendocument](https://quickstats.censusdata.abs.gov.au/census_services/getproduct/census/2016/quickstat/3?opendocument)>.

<sup>22</sup> Citing Department of Employment, Small Business and Training (Queensland), *State of Small Business 2018 report* (20 December 2018), Queensland Government publications <<https://publications.qld.gov.au/dataset/queensland-state-of-small-business/resource/fc2ff16d-b180-41db-85ae-dc3c100753af>>.

cameras, dash cameras, and other surveillance technology can be operated by any of these individuals, businesses or organisations, including children.

The scope of the stakeholders and potential complaints and respondents, is likely to be significantly larger and very different from the group OIC currently deals with. The issues are likely to be more complex. Engagement and communication will require different approaches and greater resources to reach new stakeholder groups, not previously subject to surveillance and privacy regulation. (notes omitted; notes added)

10.21 The OIC also submitted that this would involve ‘additional costs, with a potential increase in regulatory burden’, and expressed concern that the OIC ‘is not in a position to manage any additional demand placed on our services, or expansion of our functions, or nature of those functions’.<sup>23</sup>

10.22 The OIC further submitted that it does not presently have the powers and mechanisms that would be necessary to perform the functions of an independent regulator under the surveillance devices legislation. For example, it submitted that the Information Commissioner does not presently have ‘a clear power to investigate an act or practice on his or her own motion’ which would be beneficial in this context to address systemic issues.

### **The regulator’s functions and powers**

10.23 Most respondents who addressed this issue—including the Department of Agriculture and Fisheries, the Brisbane City Council, the Toowoomba Regional Council, Future Wise, the QCCL, the OIC and members of the public—submitted that the regulator under the surveillance devices legislation should have a range of regulatory and compliance functions. QAI submitted generally that ‘strong and robust’ regulatory powers would be important to give effect to the legislation.

10.24 In particular, many respondents agreed that the regulator should be responsible for conciliation or mediation of complaints,<sup>24</sup> education and best practice guidance and advice about the legislation,<sup>25</sup> and research, monitoring and reporting of matters relevant to the legislation.<sup>26</sup>

10.25 For example, Future Wise submitted that the regulator should be responsible for:

- researching and reporting on relevant matters;
- educating and issuing guidelines for surveillance practice; [and]
- educating the public on their rights

<sup>23</sup> The OIC observed in this regard that demand for its existing services, particularly for external reviews, has increased significantly since 2017–18.

<sup>24</sup> Eg, Submissions 10, 13, 15, 18, 19, 22, 25, 33, 35, 38, 39, 40, 41. See the discussion in Chapter 9 above.

<sup>25</sup> Eg, Submissions 10, 13, 15, 16, 18, 19, 22, 25, 32, 35, 38, 40, 41, 43.

<sup>26</sup> Eg, Submissions 10, 13, 15, 16, 18, 22, 25, 32, 35, 38, 40, 41, 43.

10.26 The QLS similarly submitted that the regulator's functions should include 'research and monitoring', and 'development and publishing of best practice guidelines'.

10.27 As noted at [10.6] above, an academic submitted that 'training and education, including the development of best practice guides' would be particularly helpful not only for government agencies but also for those engaged in occupations that routinely use surveillance devices and the growing numbers of people in the community using surveillance technologies like drones.<sup>27</sup>

10.28 The QCCL 'emphasised':

the importance of education in ensuring that privacy is properly understood on an informed basis and addressed without the need for the cost and resources associated with the Court's intervention.

10.29 A number of respondents also submitted that the regulator should have a role in monitoring and/or reporting on compliance with the legislation.<sup>28</sup> For example, the QLS submitted that the regulator's functions should include:

- examining the practices of individuals, corporations and others (including public authorities) in relation to their surveillance practices, and
- advising a public authority or entity about any failure to comply with laws and guidelines.

10.30 The QCCL more specifically submitted that the 'deployment' of surveillance in public places should be 'monitored' by the regulator, and that any code of conduct for surveillance by private investigators and insurers should be 'audited' by the regulator 'on a random basis'. The OIC noted that power to investigate acts or practices on the regulator's own motion can be beneficial in addressing systemic issues.

10.31 Some respondents expressed support for other investigation or enforcement powers, such as the appointment of inspectors to investigate or monitor compliance with the legislation,<sup>29</sup> the power to issue compliance notices<sup>30</sup> and the power to start civil penalty proceedings for contraventions of the legislation.<sup>31</sup> One respondent submitted that, if inspectors are appointed, they would need 'sufficient powers' including entry, warrant and seizure powers. In their view:<sup>32</sup>

These powers, alongside working with the Queensland Police Service, should provide for the satisfactory enforcement of compliance with the new laws and greater community confidence in the regulatory system.

---

<sup>27</sup> Submission 19. See also [10.6] above.

<sup>28</sup> Eg, Submissions 19, 25, 38, 40, 43.

<sup>29</sup> Eg, Submissions 13, 15, 18, 35, 38, 40, 41.

<sup>30</sup> Eg, Submissions 13, 15, 18, 22, 32, 35, 38, 40, 41.

<sup>31</sup> Eg, Submissions 13, 15, 22, 38, 40, 41.

<sup>32</sup> Submission 13.

10.32 Some respondents did not support all of these enforcement functions.<sup>33</sup> For example, the AAUS and a member of the public submitted that the regulator should refer potential criminal contraventions of the legislation to police,<sup>34</sup> and the Brisbane City Council did not support a power to start civil penalty proceedings.

10.33 One member of the public submitted that the regulator should additionally be empowered to assess and decide applications for ‘special approval’ to use a surveillance device in prescribed circumstances.<sup>35</sup>

10.34 The OIC submitted that the conferral of functions on the regulator would require appropriate resourcing:

If such functions are allocated without appropriate resourcing, it would undermine the effectiveness of, and community confidence in, a new civil surveillance regime.

10.35 The QLS noted the need to manage potential conflicts between different functions carried out by the regulator:

QLS suggests that, should an independent regulator hold dual functions such as investigatory powers, ability to refer a matter for prosecution or commence a civil penalty proceeding, these mechanisms must be carefully managed to ensure that internal measures are put in place to avoid the effects of subconscious bias which may be accumulated by an investigator. A direction that separate officers are to carry out investigation and facilitation functions is one example of such measures.

## EXISTING PROVISIONS AND PROPOSALS

10.36 The current regulatory and compliance approach of surveillance devices legislation in Australia is primarily criminal, relying on police investigation and prosecution of criminal offences.<sup>36</sup> There is provision under the *Invasion of Privacy Act 1971* for the appointment of inspectors to monitor compliance,<sup>37</sup> but these provisions are no longer used.<sup>38</sup>

---

<sup>33</sup> Eg, Submissions 18, 19, 22, 25, 35, 39, 43.

<sup>34</sup> Submission 22; and see AAUS and Liberty Victoria Paper (2015) [5.4], adopted in Submission 39 from the AAUS.

<sup>35</sup> Submission 13.

<sup>36</sup> See generally, in addition to the discussion that follows in this chapter, QLRC Consultation Paper No 77 (2018) [3.286]–[3.285], [3.308]–[3.319].

<sup>37</sup> *Invasion of Privacy Act 1971* (Qld) ss 5–7, discussed at QLRC Consultation Paper No 77 (2018) [3.309]–[3.311]. These provisions 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 the *Privacy Act 1988* (Cth) pt IIIA and the *Security Providers Act 1993* (Qld).

<sup>38</sup> 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.

10.37 There is no separate or independent regulatory body with specific oversight functions and powers in relation to the use of surveillance devices in civil society in any of the Australian jurisdictions.<sup>39</sup>

10.38 However, regulators with particular functions relating to surveillance have been established in England and Wales, and proposals for independent regulators have been made in other Australian jurisdictions. Guidance can also be drawn from existing provisions in Queensland legislation, including the IP Act and the *Human Rights Act 2019*.

## Other jurisdictions

10.39 In England and Wales,<sup>40</sup> the *Protection of Freedoms Act 2012* (UK) provides for the publication of a code of practice on the use of surveillance camera systems by relevant authorities, and the appointment of a Surveillance Camera Commissioner to encourage and monitor compliance with that code.<sup>41</sup>

10.40 Under that Act, police and local authorities must have regard to the code of practice when exercising functions to which the code relates.<sup>42</sup> Non-compliance does not itself give rise to criminal or civil liability, but may be taken into account in other proceedings.<sup>43</sup> Other users of surveillance camera systems are also encouraged to adopt the code voluntarily.<sup>44</sup>

10.41 The Surveillance Camera Commissioner's functions are to encourage compliance with the code, review the operation of the code, and provide advice about the code, including changes to it or contraventions of it. The Commissioner must report annually on the exercise of those functions to the Secretary of State.<sup>45</sup>

<sup>39</sup> Oversight of the surveillance activities of law enforcement agencies in Queensland is the responsibility of specific independent entities, including the public interest monitors appointed under the *Police Powers and Responsibilities Act 2000* (Qld) ch 21 pt 5 and the *Crime and Corruption Act 2001* (Qld) ch 6 pt 5. A similar approach is taken under the *Surveillance Devices Act 2007* (NSW) pts 3, 6 under which certain oversight functions and powers relating to surveillance device warrants may be conferred on an independent 'Surveillance Devices Commissioner'. The use of surveillance devices for State law enforcement purposes is excluded from this review: see terms of reference, para E in Appendix A.

<sup>40</sup> In the United Kingdom, the use of surveillance devices is not the subject of a single or comprehensive piece of legislation. Different aspects of surveillance are covered, to varying extents, by several regulatory regimes including the *Data Protection Act 2018* (UK) c 12, the *Regulation of Investigatory Powers Act 2000* (UK) c 23 and the *Protection of Freedoms Act 2012* (UK) c 9, pt 1 ch 1, pt 2.

<sup>41</sup> *Protection of Freedoms Act 2012* (UK) c 9, pt 2 ch 1. 'Surveillance camera systems' include CCTV and automatic number plate recognition systems: s 29(6). They also encompass body worn video, vehicle borne cameras and unmanned aerial vehicles: Surveillance Camera Commissioner, *A National Surveillance Camera Strategy for England and Wales* (March 2017) [3].

<sup>42</sup> *Protection of Freedoms Act 2012* (UK) c 9, s 33(1), (5) (definition of 'relevant authority').

<sup>43</sup> *Protection of Freedoms Act 2012* (UK) c 9, s 33(2)–(4).

<sup>44</sup> UK Government, Home Office, *Surveillance Camera Code of Practice* (June 2013) [1.2], [1.17], issued and published pursuant to the *Protection of Freedoms Act 2012* (UK) c 9, ss 30, 32, and available at <<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>>. The code sets out 12 guiding principles for surveillance camera systems in public places which are intended to ensure 'proportionality and transparency' in the use of such systems: [1.6], [2.6]. The initial focus of the legislation is on police and local authorities, but the list of 'relevant authorities' under s 33(5) of the Act may be expanded in the future: [1.8].

<sup>45</sup> *Protection of Freedoms Act 2012* (UK) c 9, ss 34(2), 35. The report is to be laid before Parliament and published.

10.42 This is intended as an 'incremental' regulatory approach to address community concerns in that jurisdiction about the use of surveillance cameras by public authorities through appropriate guidance, but 'without creating burdensome new bureaucracy'.<sup>46</sup> Over time, additional entities may become subject to the code.<sup>47</sup>

10.43 The Surveillance Camera Commissioner is assisted by a number of specialist advisory groups,<sup>48</sup> and has developed a national surveillance camera strategy to improve standards within the industry.<sup>49</sup> The Surveillance Camera Commissioner works in cooperation with the UK Information Commissioner which has responsibilities under the *Data Protection Act 2018* (UK) for personal data protection.<sup>50</sup>

10.44 The *Protection of Freedoms Act 2012* (UK) additionally provides for the appointment of a Biometrics Commissioner whose role is to keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints.<sup>51</sup> This does not apply to biometric surveillance in civil contexts.

10.45 Proposals for independent regulators under surveillance devices legislation have been made in other jurisdictions.<sup>52</sup>

10.46 For example, the NSWLRC recommended that the NSW Privacy Commissioner be given additional functions under the surveillance devices legislation to investigate and conciliate complaints about contraventions of the legislation and, in relation to 'overt' surveillance, to:<sup>53</sup>

---

<sup>46</sup> Surveillance Camera Commissioner, *Annual Report 2013–14* (December 2014) 9. And see United Kingdom, *Parliamentary Debates*, House of Commons, 1 March 2011, vol 524 col 207–09 (T May, Secretary of State for the Home Department) and House of Lords, 8 November 2011, vol 732 col 169 (Lord Henley, Minister of State, Home Office).

<sup>47</sup> United Kingdom, *Parliamentary Debates*, House of Commons, 1 March 2011, vol 524 col 207–09 (T May, Secretary of State for the Home Department) and House of Lords, 8 November 2011, vol 732 col 169 (Lord Henley, Minister of State, Home Office). See also n 44 above.

<sup>48</sup> See Surveillance Camera Commissioner, *Our governance* <<https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about/our-governance>>. The commissioner was also established with a support staff with relevant technical experience: see Surveillance Camera Commissioner, *Annual Report 2013–14* (December 2014) 11–12.

<sup>49</sup> Surveillance Camera Commissioner, *A National Surveillance Camera Strategy for England and Wales* (March 2017).

<sup>50</sup> Surveillance Camera Commissioner and Information Commissioner's Office, *Memorandum of Understanding* (30 October 2013, updated 5 September 2017 and 4 October 2019).

<sup>51</sup> *Protection of Freedoms Act 2012* (UK) c 9, pt 1 ch 1 ss 20–21, providing for the appointment and functions of the 'Commissioner for the Retention and Use of Biometric Material'. See generally GOV.UK, *Office of the Biometrics Commissioner* <<https://www.gov.uk/government/organisations/biometrics-commissioner>>.

<sup>52</sup> 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.

<sup>53</sup> NSWLRC Interim Report No 98 (2001) Recs 91–100, 105; NSWLRC Report No 108 (2005) Rec 2. The NSWLRC recommended that the surveillance devices legislation should deal with 'overt' and 'covert' surveillance differently: see NSWLRC Interim Report No 98 (2001) [10.6], [10.8] and the summary in QLRC Consultation Paper No 77 (2018) App D [D.5]–[D.7].

- promote, and provide assistance for, compliance with the proposed ‘overt surveillance principles’;
- assist surveillance users in drafting codes of practice;
- appoint inspectors to conduct routine and random inspections of surveillance systems or devices to ascertain compliance with the legislation;<sup>54</sup> and
- educate the public on the acceptable use of surveillance devices.

10.47 In their view, this would facilitate the objectives of the surveillance devices legislation and would align with the general functions of the NSW Privacy Commissioner under the *Privacy and Personal Information Protection Act 1998* (NSW).<sup>55</sup>

10.48 The VLRC similarly recommended that the surveillance devices legislation should confer functions on an independent regulator ‘to guide [the] responsible use of public place surveillance’. The regulator’s primary roles would be to provide practical guidance to surveillance users and to keep the government and the community informed of rapidly changing technology.<sup>56</sup> In particular, it recommended that the regulator should be responsible for:<sup>57</sup>

- research and monitoring, including use, technologies and current laws
- educating, providing advice and promoting understanding of laws and best practice
- developing and publishing best practice guidelines
- ...
- investigating and taking civil proceedings in relation to potential breaches of the [surveillance devices legislation]<sup>58</sup>
- 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 ... (note added)

10.49 In addition, the VLRC recommended that the regulator’s functions should include:<sup>59</sup>

---

54 With a ‘right of entry’ to non-residential premises to inspect surveillance systems or devices to ascertain compliance with the legislation: NSWLRC Report No 108 (2005) Rec 2.

55 NSWLRC Interim Report No 98 (2001) [4.67]–[4.68]. The NSWLRC’s recommendation has not been implemented.

56 VLRC Report No 18 (2010) [5.31], Rec 3.

57 Ibid Rec 4(a)–(c), (g)–(h); and see [5.41]–[5.59], [5.88]–[5.98].

58 The VLRC recommended the inclusion of civil penalties as an alternative to criminal penalties in the surveillance devices legislation, with the proposed regulator having the power to commence civil penalty proceedings. 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 such as the *Privacy Act 1998* (Cth): see *ibid* [5.95]–[5.98], [6.82]–[6.93], Recs 4(g), 19, 21.

59 Ibid Rec 4(d)–(f); and at [5.60]–[5.87].

- reviewing advice prepared by public authorities and significant private users of public place surveillance<sup>60</sup>
- 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 (note added)

10.50 In their view, public authorities who exercise the power of the State should be held to the highest standards of compliance, and significant private users would generally be able to carry the small burden of additional accountability.<sup>61</sup> The VLRC did not define ‘significant private user’ for this purpose, but proposed that it could include the following:<sup>62</sup>

- all organisations with a turnover of at least \$3 million
- all major sporting and entertainment venues
- all organisations with a primary purpose of conducting surveillance
- other organisations or classes of organisations nominated by the regulator, including those using particularly invasive forms of surveillance.

10.51 The VLRC generally preferred a facilitative rather than a punitive approach, with a focus on educating surveillance users about responsible practices and privacy protection.<sup>63</sup> It 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 members of the public about their rights if surveillance is misused, and provide valuable information to legislators.<sup>64</sup>

10.52 Similarly to the NSWLRC, it proposed that the functions of the regulator be conferred on the Victorian Privacy Commissioner. In its view:<sup>65</sup>

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.

---

<sup>60</sup> The VLRC recommended that public authorities and significant private users be required to advise the regulator annually on their compliance with public place surveillance guidelines in relation to designated surveillance devices: *ibid* Rec 5.

<sup>61</sup> *Ibid* [5.64], [5.70].

<sup>62</sup> *Ibid* [5.72]–[5.73], [5.74]–[5.76]. The VLRC considered that the government, working in conjunction with the proposed regulator, would be best placed to determine which organisations are ‘significant private users’.

<sup>63</sup> *Ibid* [5.31], [5.34], [5.36].

<sup>64</sup> See generally *ibid* [5.46] ff.

<sup>65</sup> *Ibid* (2010) [5.99]–[5.100], Rec 9. The VLRC’s recommendation has not been implemented, but see QLRC Consultation Paper No 77 (2018) App D [D.17] as to the guidelines on surveillance and CCTV that have been issued in that jurisdiction.



... 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.

10.53 The NZLC did not consider it necessary for there to be a specific regulator to monitor surveillance. However, it proposed that the Privacy Commissioner of New Zealand should be additionally empowered to report regularly to Parliament on developments in surveillance and surveillance technologies. It explained that:<sup>66</sup>

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.

## Other legislation in Queensland

10.54 Relevantly, in Queensland, the OIC is conferred with functions under the IP Act relating to information privacy obligations of Queensland government agencies.

10.55 The OIC, which consists of the Information Commissioner and the staff of the OIC, is established under the *Right to Information Act 2009* ('RTI Act').<sup>67</sup> The commissioner and the OIC are independent of government,<sup>68</sup> and the commissioner is conferred with a range of functions under both the RTI Act and the IP Act.<sup>69</sup> Those Acts are part of the public sector accountability framework.<sup>70</sup>

10.56 The IP Act also establishes the Privacy Commissioner whose 'role is that of a deputy to the Information Commissioner'. The Privacy Commissioner performs the functions under the IP Act that are delegated to him or her by the Information Commissioner.<sup>71</sup>

<sup>66</sup> NZLC Report No 113 (2010) [4.7], Rec 18.

<sup>67</sup> See *Right to Information Act 2009* (Qld) s 123 which provides for the Information Commissioner as an officer of the Parliament, and continues in existence the OIC established under the *Freedom of Information Act 1992* (Qld) (repealed). The Information Commissioner is appointed by the Governor in Council: s 134. The OIC is a statutory body: s 124.

<sup>68</sup> See *Right to Information Act 2009* (Qld) s 127; *Information Privacy Act 2009* (Qld) ss 134, 140.

<sup>69</sup> See generally *Right to Information Act 2009* (Qld) ch 4 pt 2; *Information Privacy Act 2009* (Qld) ch 4 pt 1.

<sup>70</sup> See generally Queensland Government (Department of the Premier and Cabinet), 'The Right to Information: A Response to the review of Queensland's Freedom of Information Act' (2008); OIC, *Annual Report 2009–10* (2010) 8; Queensland Government, *Ethics in the public service* (7 May 2019) <<https://www.forgov.qld.gov.au/ethics-public-service>>.

<sup>71</sup> See *Information Privacy Act 2009* (Qld) ss 141(1), 142. The Privacy Commissioner is a staff member of the OIC and is subject to the direction of the Information Commissioner: ss 141(2), 143. (Similarly, the *Right to Information Act 2009* (Qld) establishes the Right to Information Commissioner as a deputy to the Information Commissioner, and staff member of the OIC, to perform the functions under that Act that are delegated to him or her by the Information Commissioner; the Right to Information Commissioner is subject to the direction of the Information Commissioner: ss 147–149.)

10.57 Under the IP Act, the Information Commissioner has various complaints, guidance, advice, monitoring and compliance functions, including:<sup>72</sup>

- mediating privacy complaints against Queensland government agencies;<sup>73</sup>
- promoting understanding of and compliance with the privacy principles;
- providing advice and assistance to relevant entities on the interpretation and administration of the legislation;
- initiating privacy education and training, including to promote greater awareness of the operation of the legislation in the community and within the public sector environment;
- issuing guidelines, including guidelines on how the legislation should be applied and on privacy best practice generally;<sup>74</sup>
- identifying and commenting on legislative and administrative changes that would improve the administration of the legislation;
- reviewing the personal information handling practices of relevant entities, including technologies, programs, policies and procedures, to identify systemic issues (and, if appropriate, reporting on the findings of any review);<sup>75</sup>
- conducting compliance audits to assess relevant entities' compliance with the privacy principles;
- issuing compliance notices in particular circumstances;<sup>76</sup> and

<sup>72</sup> *Information Privacy Act 2009* (Qld) ss 135, 136. The Information Commissioner also has functions relating to external reviews of agency decisions under ch 3 pt 9 of the Act: s 137.

<sup>73</sup> See *Information Privacy Act 2009* (Qld) ch 5, discussed in Chapter 9 above.

<sup>74</sup> Relevantly, the Information Commissioner has issued guidelines for government agencies about privacy and the use of camera surveillance and drones: see [D.26] below. See also OIC, Information Sheet: Camera surveillance, video, and audio recording—a community guide (2019).

<sup>75</sup> A review may also be conducted to identify particular grounds for the issue of a compliance notice: *Information Privacy Act 2009* (Qld) s 135(1)(a)(i) and see n 76 below.

<sup>76</sup> See *Information Privacy Act 2009* (Qld) ch 4 pt 6 which enables the Information Commissioner to give an agency a compliance notice, requiring the agency to take stated action within a stated period, if the agency has contravened the obligation to comply with the privacy principles in a way that is 'serious or flagrant': s 158. Failure to comply with a compliance notice is an offence punishable by a fine of up to 100 penalty units (\$13 345): s 160. An agency given a compliance notice may apply to QCAT for a review of the decision: ss 161–163.

- waiving or modifying the obligation to comply with the privacy principles in particular circumstances.<sup>77</sup>

10.58 The Information Commissioner has power to do all things necessary or convenient to be done for or in connection with the performance of those functions.<sup>78</sup>

10.59 The Information Commissioner must also report annually to Parliament on the operation of the OIC under the IP Act, including details about the number and outcomes of privacy complaints received under the Act.<sup>79</sup>

10.60 At the federal level, the Australian Information Commissioner has generally similar functions in relation to information privacy matters under the Privacy Act.<sup>80</sup> However, there are some notable differences. In particular, the Australian Information Commissioner has more extensive investigative and enforcement powers, including the power to make determinations about information privacy complaints and to take proceedings to enforce civil penalty provisions under the legislation. It is also given a specific research and monitoring function of:<sup>81</sup>

undertaking research into, and monitoring developments in, data processing and technology (including data matching and linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised [and] reporting to the Minister the results of that research and monitoring

10.61 Oversight of some privacy-related matters in Queensland is also provided for under the *Human Rights Act 2019*. That Act requires public entities to act and make decisions in a way that is compatible with human rights, including the right to 'privacy and reputation'.<sup>82</sup> The Act renames the Anti-Discrimination Commission

<sup>77</sup> See *Information Privacy Act 2009* (Qld) ch 4 pt 5 which enables the Information Commissioner, on application of an agency, to approve by gazette notice a waiver or modification of the agency's obligation to comply with the privacy principles for a stated period or until the approval is revoked or amended: s 157(1)–(2). An approval may be given only if the Information Commissioner is satisfied that the public interest in the agency's compliance with the privacy principles is outweighed by the public interest in waiving or modifying the compliance to the extent stated in the approval: s 157(4). This allows for unique or unforeseen situations to be managed: see OIC, *Guidelines—Privacy Principles: Understanding the privacy principles—Power of the Information Commissioner to waive or modify the privacy principles* (19 July 2013) <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/power-of-the-information-commissioner-to-waive-or-modify-the-privacy-principles>>.

<sup>78</sup> See *Right to Information Act 2009* (Qld) s 125. See also *Information Privacy Act 2009* (Qld) s 11 sch 5 which defines 'function' to include a power. Note that 'function' includes duty, and 'power' includes authority: *Acts Interpretation Act 1954* (Qld) s 36 sch 1.

<sup>79</sup> *Information Privacy Act 2009* (Qld) s 193(2)–(3); *Information Privacy Regulation 2009* (Qld) s 5(2). The Information Commissioner reports to Parliament through the Speaker and the Legal Affairs and Community Safety Committee. See also OIC, *Meetings with the Parliamentary committee* <<https://www.oic.qld.gov.au/about/our-organisation/meetings-with-the-parliamentary-committee>>.

<sup>80</sup> See *Privacy Act 1998* (Cth) pt IV div 2, pt V, pt VIB div 1. The OAIC and the Australian Information Commissioner are established under the *Australian Information Commissioner Act 2010* (Cth).

<sup>81</sup> *Privacy Act 1998* (Cth) s 28A(2)(d)–(e).

<sup>82</sup> The *Human Rights Act 2019* (Qld) s 73(4) also provides that, if the subject matter of a complaint could be the subject of a privacy complaint under the IP Act, the Human Rights Commissioner (the 'commissioner') may refer the complaint to the Information Commissioner. See further [D.15]–[D.17] below.

Queensland as the Queensland Human Rights Commission ('QHRC')<sup>83</sup> and confers a range of functions on the Human Rights Commission, including:<sup>84</sup>

- conciliating human rights complaints against public entities;
- promoting an understanding and acceptance, and the public discussion, of human rights and the *Human Rights Act 2019* in Queensland;
- making information about human rights available to the community;
- providing education about human rights and the Act;
- advising the Attorney-General about matters relevant to the operation of the Act;
- assisting the Attorney-General in reviews of the Act;
- if asked by the Attorney-General, reviewing the effect of other Acts, statutory instruments and the common law on human rights and reporting to the Attorney-General on the outcome of the review; and
- reviewing public entities' policies, programs, procedures, practices and services in relation to their compatibility with human rights.

10.62 The Human Rights Commissioner must also report annually to the Attorney-General on the operation of the Act, including information about human rights complaints made or referred under the Act.<sup>85</sup>

10.63 The functions of other regulatory bodies in Queensland do not specifically relate to privacy or surveillance in civil society, although such matters might arise indirectly.<sup>86</sup> For example, a health service complaint to the Health Ombudsman might relate to the disclosure of a person's health information.<sup>87</sup>

---

<sup>83</sup> See *Human Rights Act 2019* (Qld) (as passed) ss 118, 124, replacing s 234 and the definitions of 'commission' and 'commissioner' in the *Anti-Discrimination Act 1991* (Qld). The QHRC is a statutory body and the commissioner is appointed by the Governor in Council: see *Anti-Discrimination Act 1991* (Qld) ss 237A, 238(1).

<sup>84</sup> *Human Rights Act 2019* (Qld) s 61. See also s 62 as to the commissioner's power to do all things necessary or convenient to be done for the performance of the commission's functions under that Act. Under that Act, 'function' is defined to include a 'power': s 6 sch 1.

<sup>85</sup> *Human Rights Act 2019* (Qld) s 91. The commissioner may also report about matters relevant to the commissioner's functions on the commissioner's own initiative, and must do so if requested by the Attorney-General: s 92.

<sup>86</sup> See, eg, the Ombudsman established under the *Ombudsman Act 2001* (Qld) pt 2 which has responsibility for investigating the administrative actions of government departments, local governments and public authorities; and the Health Ombudsman established under the *Health Ombudsman Act 2013* (Qld) pt 2 which has responsibility for complaints and investigations about health services.

<sup>87</sup> See generally Office of the Health Ombudsman, *What can I complain about?* (2020) <<https://www.oho.qld.gov.au/health-consumers/what-can-i-complain-about/>>.

## THE COMMISSION'S VIEW

10.64 In the Commission's view, there is a clear need for an independent regulatory body.

10.65 The ubiquity and intrusive nature of surveillance device technologies, their potential to infringe and intrude upon individuals' privacy and the growing significance of these issues in people's lives require an appropriate regulatory response.

10.66 Especially in the context of civil society—where surveillance devices are used by ordinary members of the public as well as organisations, businesses and government agencies—an independent body is required to help the community understand and give effect to their responsibilities and rights under the legislation. The oversight and expertise of an independent regulator will give practical effect to the protective intent of the legislation. It will also align with one of the objectives of the Queensland Drones Strategy, to 'support community-friendly drone policies', by providing a clear avenue for information and redress.<sup>88</sup>

10.67 The regulator will need to work with, and provide leadership to, both government and non-government entities and individuals across civil society. Because the draft Bill applies to all persons, including the State, it is essential that the regulator is independent of government. This will ensure impartiality, fairness and transparency, will maintain stability and a consistent focus, and will enhance community confidence in the regulator and the legislation.

10.68 The independent regulator will provide an additional mechanism for dealing with possible infringements through a complaints handling function, as well as an avenue for education, expert advice, monitoring and best practice guidance.

10.69 The Commission recognises that the establishment of an independent regulator will have resource implications, but considers that the public interest and benefits of doing so should justify the financial cost.

### Which entity

10.70 The independent regulator could be established by conferring its functions on an existing entity, or by creating a new, separate entity for this purpose. This is properly a question for government, taking into account public policy and resource implications.

### *Conferring the functions on the OIC or the QHRC*

10.71 None of the existing regulatory entities in Queensland is an ideal fit in this context.

10.72 One option is to expand the existing role of the Information Commissioner. Both the IP Act and the draft Bill relate to aspects of privacy (albeit to differing extents

---

<sup>88</sup> QDS (2018) 31. Objective 4 'aims to balance industry growth with community-friendly outcomes', including by protecting individual rights such as privacy. One of the opportunities identified by the QDS is to address privacy concerns, including the difficulty of navigating the 'privacy landscape', while 'ensuring a regulatory environment that fosters investment and industry development': 15.

and in different contexts), and some of the Information Commissioner's functions under the IP Act<sup>89</sup> are analogous to those the Commission recommends in this chapter.

10.73 The preferred structure might be for the draft Bill to confer the functions under the legislation on the Information Commissioner and to establish a new office-holder, to whom the performance of some or all of those functions would be delegated. This would mirror the general approach taken to the RTI Commissioner under the RTI Act and the Privacy Commissioner under the IP Act.<sup>90</sup>

10.74 A second option is to extend the role of the Human Rights Commissioner. The right to 'privacy and reputation' is one of several matters for which the Human Rights Commissioner has complaints handling and reporting functions under the *Human Rights Act 2019*.<sup>91</sup> The Human Rights Commissioner also has complaints handling functions, with similar features to those recommended in this chapter for the proposed independent regulator, under the *Anti-Discrimination Act 1991*.<sup>92</sup>

10.75 Again, the preferred structure might be to confer the proposed functions on the Human Rights Commissioner and to establish a new office-holder to whom the performance of some or all of those functions would be delegated.<sup>93</sup>

10.76 Each of those two options would have the advantage of placing the regulator within an established and recognised agency. That might allow for some existing resources and procedures to be shared within the relevant existing agency. Sufficient additional resources would still be required to enable the independent regulator to operate effectively, as would the internal separation of different functions under different legislative frameworks.<sup>94</sup> Depending on the terms of the agency's existing statutory framework, there is also need to provide for specific operational matters, including the terms of office of any new office-holder, protections and offences in

---

89 See [10.54]–[10.59] above.

90 See [10.55]–[10.56] above.

91 See [10.61] above.

92 See generally *Anti-Discrimination Act 1991* (Qld) ch 7 pt 1.

93 At present, the Human Rights Commissioner is assisted in the performance of its functions under the *Anti-Discrimination Act 1991* (Qld) and the *Human Rights Act 2019* (Qld) by a 'deputy commissioner'. That office is not separately established by the legislation. However, the commissioner is empowered to delegate functions or powers under those Acts to another person: *Anti-Discrimination Act 1991* (Qld) s 244(a).

94 See the OIC, *Office of the Information Commissioner Queensland Organisational Chart* (2019) <[https://www.oic.qld.gov.au/\\_data/assets/pdf\\_file/0019/7714/corporate\\_oic\\_org-chart.pdf](https://www.oic.qld.gov.au/_data/assets/pdf_file/0019/7714/corporate_oic_org-chart.pdf)> which includes separate teams for the RTI Commissioner's external review functions and the Privacy Commissioner's privacy functions; and the Queensland Human Rights Commission, *Organisational Chart* (22 July 2019) <[https://www.qhrc.qld.gov.au/\\_data/assets/pdf\\_file/0016/20590/2019.08.13-Organisational-structure.pdf](https://www.qhrc.qld.gov.au/_data/assets/pdf_file/0016/20590/2019.08.13-Organisational-structure.pdf)> which includes separate teams for the Commissioner's community relations, complaint management and human rights policy and research functions.

dealings with the independent regulator under the legislation, and reporting obligations.<sup>95</sup> Consequential amendments to other Acts might also be required.<sup>96</sup>

10.77 Both the OIC and the QHRC have particular privacy-related functions. However, there are key points of difference with the regulation of surveillance devices under the draft Bill:

- The draft Bill regulates the civil use of surveillance devices by members of the community. In contrast, the IP Act and the *Human Rights Act 2019* primarily apply only to the acts and practices of government agencies and public entities and are part of the law governing public service administration, which has a different and narrower focus on public sector accountability.
- The wider scope of the draft Bill will involve a much greater number of stakeholders as well as a diverse range of issues and considerations. Expectations and considerations will differ between government agencies and, for example, neighbours, community groups, small and large businesses, and different occupational groups.
- Further, the draft Bill has a significant criminal component and will rely in that respect on police investigation and prosecution of offences. In contrast, the IP Act and the *Human Rights Act 2019* are primarily administrative schemes that are not framed around criminal offences.

10.78 The independent regulator under the draft Bill will also need specialist knowledge and expertise covering several different aspects of privacy in relation to the use of surveillance devices, such as territorial privacy and locational or tracking privacy,<sup>97</sup> as well as the nature, use and implications of current and emerging surveillance device technologies. This is a different focus and area of specialisation to that of the OIC or the QHRC.

10.79 The conferral of functions on either of those entities would significantly expand and change the nature of their roles. This is likely to have resource implications for those entities, and could potentially have an adverse impact on their existing responsibilities.<sup>98</sup> Whilst it might be expected that progress toward a more comprehensive, coordinated (and national) privacy and data protection scheme would be made in the future, this is not presently the case and is beyond the scope of the current review.<sup>99</sup>

---

<sup>95</sup> For example, some provisions of the *Right to Information Act 2009* (Qld) about the establishment of the Information Commissioner are of general application, but other provisions dealing with operational matters under both the *Right to Information Act 2009* (Qld) and the *Information Privacy Act 2009* (Qld) apply only for the purposes of those Acts.

<sup>96</sup> For example, the *Right to Information Act 2009* (Qld) s 144 provides that staff of the OIC must be employed under the *Public Service Act 2008* (Qld) but that this does not apply to the RTI Commissioner or the Privacy Commissioner. Consideration would be needed as to whether the same approach should be taken if a new deputy to the Information Commissioner were to be created under the surveillance devices legislation.

<sup>97</sup> See [2.8] ff above as to the various privacy interests that may arise, in addition to and distinct from information privacy.

<sup>98</sup> See, eg, the OIC at [10.21] above.

<sup>99</sup> See also [3.43] above.

10.80 In this regard, the Commission also observes that the proposals in other jurisdictions to confer functions under surveillance devices legislation on the Privacy Commissioners of NSW and Victoria have not been implemented.<sup>100</sup>

### ***Creating a new, separate entity***

10.81 A third option is for the draft Bill to provide for the establishment of a new, separate independent regulator. This would involve the creation of a new standalone office and appointment of the office-holder with responsibility for the functions under the legislation.

10.82 This approach would have the advantage of tailoring the provisions and establishing a purpose-specific regulator with a clear role and separation of functions from other entities. The draft Bill would provide for all relevant operational matters, and there would be a reduced need for amendments to other Acts.

10.83 The establishment of a separate independent regulator is not without precedent, as indicated by the establishment in England and Wales of the Surveillance Camera Commissioner as part of an incremental approach to surveillance regulation in that jurisdiction.<sup>101</sup> This recognises the particular challenges posed by surveillance, as distinct from other, albeit related, issues of information privacy and data protection.

10.84 This approach will involve establishment costs for the new independent regulator and would require sufficient resources to enable it to operate effectively.

### ***The approach of the draft Bill***

10.85 As stated above, the decision as to whether the independent regulator should be established as a new entity or by the conferral of functions on an existing entity is properly a matter for government.

10.86 For the purpose of giving practical effect to the Commission's recommendations in this chapter, and to provide a complete legislative framework, the draft Bill is framed on the third option of a new, separate independent regulator. The Commission has taken this approach in order to provide a clear picture of the functions and powers to be conferred upon the recommended independent regulator.

10.87 If the independent regulator's functions and powers were, alternatively, to be conferred on an existing entity, some of the provisions of the draft Bill would need appropriate modification to ensure they are able to achieve the same substantive effect whilst taking into account the existing entity's current legislative and operational structure.<sup>102</sup>

---

<sup>100</sup> See [10.46]–[10.52] above.

<sup>101</sup> See [10.39]–[10.43] above.

<sup>102</sup> See also [10.76] above.



10.88 Whichever approach to establishment is taken, the independent regulator should have the functions, powers and other main features outlined in this chapter and must be adequately resourced to perform its functions effectively.

## ELEMENTS OF THE RECOMMENDED APPROACH

### Establishment of the regulator

#### *Statutory body*

10.89 The draft Bill provides for a Surveillance Devices Commission (the 'commission'), consisting of the Surveillance Devices Commissioner (the 'commissioner') and the staff of the commission.

10.90 Consistently with other legislation,<sup>103</sup> the draft Bill provides that the commission is a statutory body for the *Financial Accountability Act 2009* and the *Statutory Bodies Financial Arrangements Act 1982*. This will ensure that the commission has adequate and appropriate financial powers and accountability obligations, including the requirement to prepare annual financial statements for audit and tabling in Parliament.<sup>104</sup>

#### *Appointment of commissioner*

10.91 The draft Bill provides for the appointment of the commissioner, under the legislation, by the Governor in Council for a term of not more than five years. It further provides that a person may not be reappointed as commissioner if it would result in the person holding office as commissioner for more than ten years continuously.<sup>105</sup> This will balance the need for continuity, with the benefit of diversity.

10.92 Except as otherwise provided by the draft Bill, the commissioner is to hold office on the terms and conditions, including as to remuneration and allowances, decided by the Governor in Council.

10.93 Consistently with other legislation,<sup>106</sup> the draft Bill also provides for the inclusion of other standard provisions about the commissioner's appointment and conditions, including leave of absence as commissioner, vacancy in office (including resignation), the grounds on which a person may be removed from office as commissioner,<sup>107</sup> and the preservation of certain rights of public service employees.

10.94 In accordance with provisions of general application under the *Acts Interpretation Act 1954*, the Governor in Council may also appoint a person to act as

<sup>103</sup> See, eg, *Right to Information Act 2009* (Qld) s 124; *Anti-Discrimination Act 1991* (Qld) ss 237, 237A.

<sup>104</sup> As to annual financial statements and reporting requirements of statutory bodies, see *Financial Accountability Act 2009* (Qld) ss 61(d), 62, 63.

<sup>105</sup> See, in similar terms, *Right to Information Act 2009* (Qld) s 136(2). See also, eg, *Ombudsman Act 2001* (Qld) s 61; *Legal Profession Act 2007* (Qld) s 585.

<sup>106</sup> See, eg, *Right to Information Act 2009* (Qld) ss 138, 139, 141, 142, 159–164; *Anti-Discrimination Act 1991* (Qld) ss 240, 241, 242, 243.

<sup>107</sup> See also *Acts Interpretation Act 1954* (Qld) s 25(1)(b)(i), (iii), (2) as to the implied incidental power to remove or suspend a person appointed to an office.

the commissioner during a vacancy in the office, or if the commissioner is absent or otherwise unable to discharge the functions of the office.<sup>108</sup>

### ***Independence of the commissioner***

10.95 As explained above, the Commission considers the regulator under the draft Bill should be independent of government.

10.96 Consistently with other legislation, the draft Bill provides that, in performing the commissioner's functions, the commissioner must act independently, impartially and in the public interest.<sup>109</sup> It also provides that the commissioner is not subject to direction by any person about the way in which the commissioner's functions under the draft Bill are to be performed.<sup>110</sup> (The Minister may, however, request advice, assistance or an examination, and may require a report, about particular matters.)<sup>111</sup>

### ***Delegation***

10.97 Consistently with other legislation,<sup>112</sup> the draft Bill provides that the commissioner may delegate the commissioner's functions or powers to a staff member of the commission. Given the nature of the functions conferred on the commissioner under the draft Bill, particularly in relation to the mediation of complaints, the Commission considers it desirable for the draft Bill to specify that the delegation must be to an 'appropriately qualified' staff member.<sup>113</sup>

10.98 Provisions of general application under the *Acts Interpretation Act 1954* apply to the delegation, including provisions to the effect that the delegation may be general or limited, the delegation must be in or evidenced by writing, and a delegated function or power may be exercised only in accordance with any conditions to which the delegation is subject.<sup>114</sup>

### ***The commission and its staff***

10.99 The draft Bill provides that the commissioner controls the commission.<sup>115</sup>

<sup>108</sup> See *Acts Interpretation Act 1954* (Qld) s 25(1)(b)(ii), (iv), (v).

<sup>109</sup> See, eg, *Health Ombudsman Act 2013* (Qld) s 27.

<sup>110</sup> Cf *Right to Information Act 2009* (Qld) s 126; *Information Privacy Act 2009* (Qld) s 134; *Ombudsman Act 2001* (Qld) s 13.

<sup>111</sup> See [10.113], [10.127]–[10.128] below.

<sup>112</sup> See, eg, *Information Privacy Act 2009* (Qld) s 139; *Anti-Discrimination Act 1991* (Qld) s 244.

<sup>113</sup> 'Appropriately qualified' is defined, for a function or power, to mean having the qualifications, experience or standing appropriate to perform the function or exercise the power: *Acts Interpretation Act 1954* (Qld) s 36 sch 1.

See Office of Queensland Parliamentary Counsel, *Fundamental Legislative Principles: The OQPC Notebook* (2008) [2.7.1], [2.7.2] in which it is suggested that, if significant powers are delegated to a broad category of people, legislation should require the delegate to be 'appropriately qualified'. A power is considered significant in this context if it is extensive, may affect the rights or legitimate expectations of others, or appears to require particular expertise or experience.

<sup>114</sup> See *Acts Interpretation Act 1954* (Qld) s 27A.

<sup>115</sup> Cf *Right to Information Act 2009* (Qld) s 127; *Ombudsman Act 2001* (Qld) s 74.

10.100 Consistently with other legislation, it provides for staff of the commission to be employed under the *Public Service Act 2008*.<sup>116</sup> This will ensure that staff are governed by the same general public service principles relating to employment and work performance as other public service employees.<sup>117</sup>

10.101 The draft Bill further provides that the staff of the commission are not subject to direction, other than from the commissioner or a person authorised by the commissioner, about the performance of the commissioner's functions under the legislation.<sup>118</sup> This will further ensure the independence of the new regulator.

## Functions and powers

10.102 In the Commission's view, the independent regulator's functions and powers under the draft Bill should focus on encouraging compliance with and enhancing community understanding of the legislation. The independent regulator's primary functions should be to provide education and best practice guidance, and to monitor the operation of and compliance with the legislation and developments in surveillance devices technology, together with a complaints receiving, management and mediation function. This will provide a flexible and facilitative approach, with the independent regulator taking a leadership position, but it does not include the prosecution of offences.

10.103 The Commission considers it appropriate that offences under the draft Bill for contravention of the use prohibitions or the communication or publication prohibitions are a matter for police investigation and prosecution, as is presently the case under the *Invasion of Privacy Act 1971*. The Commission does not recommend provision for a regime of civil penalty proceedings, as an alternative to prosecution of the offences.<sup>119</sup> It is not, therefore, necessary for the independent regulator to have power to investigate those offences under the draft Bill.

## General functions and powers

10.104 The draft Bill provides that the commissioner has the functions and powers given by the legislation.<sup>120</sup> Consistently with other legislation, the commissioner also has power to do all things that are necessary or convenient to perform the commissioner's functions under the legislation.<sup>121</sup>

10.105 In addition, the draft Bill empowers the commissioner to ask or direct a person, by written notice, to give information (including a document) within the

<sup>116</sup> See, eg, *Right to Information Act 2009* (Qld) s 144(1); *Anti-Discrimination Act 1991* (Qld) s 246.

<sup>117</sup> This will include, for example, the operation of standard provisions in the *Public Service Act 2008* (Qld) ss 26B(4) and 26C regarding the protection of State employees from civil liability for engaging in conduct in an official capacity.

<sup>118</sup> Cf *Information Privacy Act 2009* (Qld) s 140. See also, eg, *Ombudsman Act 2001* (Qld) s 75.

<sup>119</sup> See [3.23]–[3.25], [3.27], [5.111] ff, [5.235] ff, [6.52] ff, [6.67] ff above.

<sup>120</sup> Under the *Acts Interpretation Act 1954* (Qld), 'function' is defined to include duty, and 'power' is defined to include authority: s 36 sch 1.

<sup>121</sup> See, eg, *Right to Information Act 2009* (Qld) s 125; *Anti-Discrimination Act 1991* (Qld) s 236(2); *Human Rights Act 2019* (Qld) s 62.

reasonable period stated in the notice.<sup>122</sup> The commissioner may give such a notice if the commissioner believes on reasonable grounds that the person may have information relevant to a complaint being dealt with by the commissioner or to another function being performed by the commissioner.<sup>123</sup>

10.106 These provisions will ensure that the commissioner has sufficient powers to perform their functions.

### ***Complaints handling function***

10.107 The draft Bill provides that the commissioner's functions include receiving and dealing with complaints ('surveillance device complaints') under Part 4 of the draft Bill.<sup>124</sup> The complaints mechanism under the draft Bill, including the commissioner's obligations and powers in receiving, mediating and referring complaints, is discussed in Chapter 9 above. As noted in that chapter, the Commission considers that the complaints mechanism will provide a practical and meaningful protection for individual privacy in relation to the use of surveillance devices in civil society. It will be one of the principal functions of the commissioner.

10.108 To ensure integrity and avoid potential conflicts of interests, there should be a clear administrative division, supported by formal policies and procedures, between the complaints handling, mediation and other functions of the commissioner.<sup>125</sup> It would not be appropriate, for example, for the officer who mediates a complaint to be the same officer who provides assistance to potential complainants or who is involved in monitoring the compliance of relevant entities against whom a complaint is made.<sup>126</sup>

### ***Guidance functions***

10.109 The draft Bill provides that the commissioner has the following guidance functions:

- promoting understanding of and compliance with the legislation, including the general obligations in Part 3 of the draft Bill;
- providing information and guidance about the operation of the legislation;

<sup>122</sup> Under the draft Bill, 'information' is defined to include a record in any form and a document.

<sup>123</sup> Cf *Information Privacy Act 2009* (Qld) s 197(1)–(3); *Right to Information Act 2009* (Qld) s 103(1)–(2); *Human Rights Act 2019* (Qld) s 78(1)–(3), (9). Non-compliance with a notice is an offence: see [10.144] below. A 'complaint' under the draft Bill is defined as a 'surveillance device complaint'.

<sup>124</sup> Cf *Information Privacy Act 2009* (Qld) s 136(d); *Human Rights Act 2019* (Qld) s 61(a). See also, eg, NSWLRC Interim Report No 98 (2001) Rec 91, at [10.46] above.

<sup>125</sup> See, eg, the organisational structures of the OIC and the QHRC at <[https://www.oic.qld.gov.au/\\_data/assets/pdf\\_file/0019/7714/corporate\\_oic\\_org-chart.pdf](https://www.oic.qld.gov.au/_data/assets/pdf_file/0019/7714/corporate_oic_org-chart.pdf)> and <https://www.qhrc.qld.gov.au/about-us/our-structure>>. See also, eg, PricewaterhouseCoopers, 'Strategic Review of the Office of the Information Commissioner' (Report, 26 April 2017) [3.2.2], Rec (e).

<sup>126</sup> See the Submission from the QLS at [10.35] above.

- providing education and training about the legislation, including the general obligations in Part 3 of the draft Bill and the lawful use of surveillance devices;
- issuing guidelines about any matter related to the commissioner's functions, including guidelines on any of the following matters:
  - how the legislation applies;
  - how an exception to a prohibition in Part 2 or a general obligation in Part 3 of the draft Bill applies, including examples;
  - best practice for the use of surveillance devices, and the communication or publication of surveillance information, in a way that respects individuals' privacy;<sup>127</sup> and
  - making, referring and dealing with complaints under Part 4 of the draft Bill; and
- giving information and reasonable help to complainants and respondents in relation to their complaints and the processes under the legislation.<sup>128</sup>

10.110 The draft Bill provides that guidelines issued by the commissioner must be published on the commissioner's website.

10.111 These functions draw on similar provisions in other rights-based legislation, including the IP Act.<sup>129</sup> They will support the commissioner's primary role in providing best practice leadership to encourage compliance with the legislation. In particular, the publication of guidelines on the legislation will provide practical assistance to those seeking to use, or communicate or publish information obtained from the use of, a surveillance device.

10.112 The educative and guidance role would be to provide information and general advice about how the legislation applies, consistently with the commissioner's specialist knowledge and expertise. It is not, however, intended that the commissioner would provide specific legal advice<sup>130</sup> or make binding legal determinations.<sup>131</sup>

<sup>127</sup> Under the draft Bill, 'surveillance information' is defined to mean information obtained, directly or indirectly, using a surveillance device.

<sup>128</sup> See also [9.61], Rec 9-6 above as to the requirement for the regulator to 'give reasonable help' to an individual complainant to put the complaint in writing.

<sup>129</sup> See, eg, *Right to Information Act 2009* (Qld) ss 128(1)(a), (b), (c), (d), 132(1)–(2); *Information Privacy Act 2009* (Qld) s 135(1)(b)(i), (ii), (iv), (c), (d); *Human Rights Act 2019* (Qld) s 61(d), (f); *Anti-Discrimination Act 1991* (Qld) s 235(d), (i); *Privacy Act 1988* (Cth) s 28(1)(a), (c), (d). See also VLRC Report No 18 (2010) Rec 4 at [10.49] above.

<sup>130</sup> This is consistent with the approach taken, for example, by the OIC: see generally OIC, *Disclaimer* (2019) <<https://www.oic.qld.gov.au/disclaimer>>.

<sup>131</sup> As policy, guidelines do not have the force of law unless the empowering legislation provides that they are binding: see, eg, *Smoker v Pharmacy Restructuring Authority* (1994) 53 FCR 287, 298–301 (Hill J). A court may nevertheless have respectful regard for the opinion of an expert body in forming its own judgment or opinion: see generally S Gageler, 'Deference' (2015) 22 *Australian Journal of Administrative Law* 151, 152. See also, eg, *JL v Queensland Police Service* [2014] QCAT 623, [131]–[134] (Senior Member O'Callaghan) in which it was stated that 'the guideline is only that and could not limit or define what the legislation means'.

### **Research, advice and monitoring functions**

10.113 The draft Bill provides that the commissioner has the following research, advice and monitoring functions:<sup>132</sup>

- undertaking or commissioning research to monitor:
  - whether the legislation is achieving its purpose;
  - how surveillance devices and surveillance device technologies are used in civil society; and
  - developments in surveillance device technology;
- identifying and commenting on issues relating to the use of surveillance devices in civil society, and the communication or publication of surveillance information;
- identifying and commenting on legislative and administrative changes that would improve the operation of the legislation;
- on request of the Minister or on the commissioner's own initiative, advising the Minister about matters relevant to the operation and administration of the legislation;
- on request of the Minister, assisting the Minister to review the legislation (under clause 95 of the draft Bill);<sup>133</sup> and
- on request of the Minister, examining other Acts and proposed legislation to determine whether they are, or would be, consistent with the purpose of the legislation and the general obligations in Part 3 of the draft Bill.<sup>134</sup>

10.114 These functions—together with the reporting requirements outlined at [10.123]–[10.132] below—are of particular importance in giving ongoing effect to the draft Bill and its purpose. One of the key challenges in legislating to regulate the use of surveillance devices in civil society is the rapid development of new technologies and their widespread use. Research and monitoring of those developments and of the operation of the legislation is necessary to ensure the continued effectiveness of the legislation. The proposed new commissioner will be ideally placed to carry out these functions and in so doing to assist government in identifying improvements to

<sup>132</sup> This draws on similar provisions in other legislation: see, eg, *Right to Information Act 2009* (Qld) s 128(1)(e), (f), (g); *Information Privacy Act 2009* (Qld) s 135(1)(b)(v), (vi); *Human Rights Act 2019* (Qld) s 61(b), (g), (h); *Anti-Discrimination Act 1991* (Qld) s 235(c); *Privacy Act 1988* (Cth) ss 28A(2)(a), (d), 28B(1)(a). See also VLRC Report No 18 (2010) Rec 4 at [10.48] above.

<sup>133</sup> See Chapter 11, Rec 11-2 below as to the requirement to review the effectiveness of the legislation within five years of its commencement.

<sup>134</sup> For example, a proposed provision in another Act might purport to give an entity an unnecessarily wide discretion to use a surveillance device in particular circumstances, when a narrower provision would achieve the same purpose and be less intrusive of individual privacy. See Chapter 5 above as to when the use of a surveillance device authorised under another Act is permitted under the draft Bill.

the legislative framework. These functions will also complement the compliance monitoring functions outlined at [10.115]–[10.122] below.

### **Compliance monitoring functions**

10.115 The draft Bill provides that the commissioner also has the following compliance monitoring function:

- on the commissioner’s own initiative or otherwise, examining the practices of relevant entities, in relation to the following matters, to monitor whether the practices comply with the legislation:
  - how the entities use surveillance devices, and communicate or publish surveillance information;
  - the surveillance device, and communication or publication, technologies used by the entities; and
  - the programs, policies and procedures of the entities in relation to each of those matters.

10.116 The word ‘examine’ is to be given its ordinary meaning, namely, to inspect or scrutinise carefully; to inquire into or investigate.<sup>135</sup>

10.117 This function is an important corollary to the other monitoring functions outlined at [10.113] above, and is consistent with approaches taken or recommended elsewhere.<sup>136</sup> It will enable the commissioner, on its own initiative, to monitor the compliance of surveillance device users with the legislation and, in turn, to identify systemic issues relating to the operation of the legislation.<sup>137</sup> The reporting requirements and safeguards outlined at [10.123]–[10.132] below will apply.

10.118 It would be impractical and unduly burdensome for the commissioner to monitor compliance by every person who is subject to the draft Bill. It is intended that a ‘relevant entity’ for this function would be limited to specific types of surveillance users or areas of activity, including local and State government agencies and other entities performing functions of a public nature, and private sector organisations or individuals who regularly or routinely use or publish information from surveillance devices. In particular, it applies to:

<sup>135</sup> *Macquarie Dictionary* (online, 2019) (definition of ‘examine’, para 1).

<sup>136</sup> See, eg, *Right to Information Act 2009* (Qld) s 131(1)(a); *Information Privacy Act 2009* (Qld) s 135(1)(a)(i), (b)(iii); *Human Rights Act 2019* (Qld) s 61(c); *Privacy Act 1988* (Cth) s 40(2); and VLRC Report No 18 (2010) Rec 4 at [10.49] above. See also [10.46], [10.57], [10.61] above.

<sup>137</sup> In the context of the IP Act, it has been recognised that an ‘own motion’ power to investigate an act or practice, whether or not a complaint has been made, would be beneficial to identify and address systemic issues: see, eg, Department of Justice and Attorney-General (Queensland), ‘Review of the *Right to Information Act 2009* and *Information Privacy Act 2009*’ (Report, October 2017) 43–4. It was recommended in that review that the *Information Privacy Act 2009* (Qld) be amended to make it clear that the Information Commissioner has this power: Rec 19.

- a ‘public entity’ within the meaning of the *Human Rights Act 2019*,<sup>138</sup>
- an entity with an annual turnover of more than \$5 million for the current or previous financial year;<sup>139</sup>
- an entity that uses a surveillance device, or communicates or publishes surveillance information, on a regular or routine basis (including, for example, security providers and investigative journalists); and
- an entity that uses a surveillance device to monitor crowds in places that are open to or used by the public, whether or not on the payment of a fee (including, for example, major sporting and entertainment venue operators).<sup>140</sup>

10.119 This is similar to the approach recommended by the VLRC in relation to public place surveillance.<sup>141</sup> The draft Bill also provides for other entities to be prescribed by regulation for the purpose of this provision.

10.120 The provision does not apply, however, to the Queensland Police Service, the Crime and Corruption Commission or other entity to the extent its practices relate to enforcing a law of the State.<sup>142</sup>

10.121 It is anticipated that many relevant entities would request the commissioner’s review of their practices to ensure their compliance and identify areas for improvement, but that the commissioner would also initiate reviews without such a request. For example, reviews might be conducted randomly or where the commissioner has received multiple complaints about the same entity.

10.122 The focus of this provision is not, however, punitive. The commissioner is not empowered to issue compliance notices or to take proceedings to prosecute a contravention of the criminal prohibitions. The Commission considers the more effective approach, particularly under a new legislative framework, is to take a facilitative and monitoring role.

<sup>138</sup> See *Human Rights Act 2019* (Qld) ss 9, 10. A ‘public entity’ includes government agencies and departments (see *Public Service Act 2008* (Qld) s 24), public service employees, local governments and local government councillors and employees, the Queensland Police Service, and State Government Ministers: s 9(1). It also includes particular entities when they are performing functions of a public nature: s 9(1)(f), (h), (2)(a). See generally QHRC, *What is a public entity?* <<https://www.qhrc.qld.gov.au/your-rights/human-rights-law/what-is-a-public-entity>>.

<sup>139</sup> This \$5 million threshold is higher than the \$3 million threshold that determines whether a private sector organisation is an ‘APP entity’ subject to the provisions of the *Privacy Act 1988* (Cth), but is lower than the \$10 million threshold that determines whether an entity is a ‘small business entity’ for the purpose of certain concessions under the *Income Tax Assessment Act 1997* (Cth). See *Privacy Act 1988* (Cth) ss 6C(1), 6D; and *Income Tax Assessment Act 1997* (Cth) pt 3-45, s 328.110.

<sup>140</sup> The reference to a place open to or used by the public, whether or not on the payment of a fee, is in the same terms as para (a) of the definition of ‘public place’ in the *Summary Offences Act 2005* (Qld) s 3 sch 2.

<sup>141</sup> See [10.49]–[10.50] above.

<sup>142</sup> The use of surveillance devices for State law enforcement purposes is excluded from this review: see terms of reference, p 1, para E in Appendix A.



## Reporting requirements

10.123 The draft Bill includes a number of reporting requirements. These are an essential transparency, integrity and accountability mechanism. They are also an important adjunct to the commissioner's other functions. In particular, they are integral to the commissioner's research, advice, monitoring and compliance monitoring functions.

10.124 In addition to the annual financial reporting requirements that will apply under the *Financial Accountability Act 2009*,<sup>143</sup> the draft Bill requires the commissioner to give the Minister an annual report about the operation of the legislation, as soon as practicable after the end of each financial year. Without limiting this, the annual report is to include information for the financial year about the following matters relating to complaints made or referred to the commissioner under the draft Bill:<sup>144</sup>

- the number of complaints;
- the types of complaints, including:
  - the categories of entities to which the complaints relate;
  - the uses of surveillance devices to which the complaints relate;
  - the provisions of Part 3 of the draft Bill to which the complaints relate;
- the outcome of complaints, including:
  - the number of complaints the commissioner refused to deal with, or to continue to deal with, and the grounds for refusing (under clause 48 of the draft Bill);
  - the number and type of complaints referred by the commissioner to another entity (under clause 51 of the draft Bill);
  - the number and type of complaints resolved by the commissioner by mediation (under clause 54 of the draft Bill);
  - the number and type of complaints referred by the commissioner to QCAT (under clause 62 of the draft Bill);
- the outcome of complaints referred to QCAT;
- another matter prescribed by regulation.

---

<sup>143</sup> See [10.90], n 3 above.

<sup>144</sup> See Chapter 9 above as to the features of the complaints mechanism.

10.125 This will ensure a high quality and consistent level of reporting for each financial year. Similar reporting requirements are also imposed in other legislation.<sup>145</sup>

10.126 The Minister is required to table a copy of the annual report in the Legislative Assembly within 14 sitting days after receiving the report.<sup>146</sup>

10.127 The draft Bill also provides that the commissioner may at any time prepare a report about a matter relevant to the performance of the commissioner's functions under the legislation and give the report to the Minister. Additionally, if asked by the Minister, the commissioner must prepare such a report and give it to the Minister as soon as practicable after it is prepared. The Minister must table a copy of a report given under these provisions in the Legislative Assembly within 14 sitting days after receiving the report.<sup>147</sup>

10.128 This will ensure that, for example, where the Minister has requested advice about matters relevant to the operation of the draft Bill or an examination of the consistency of other Acts with the draft Bill, those matters are the subject of a formal and public report.<sup>148</sup> It will also enable the commissioner to formally report on other significant matters, including the results of research, and systemic issues identified in compliance reviews.<sup>149</sup>

10.129 The draft Bill also includes particular safeguards for reports prepared under these provisions.

10.130 It provides that a report of the commissioner must not include personal information about an individual unless the information has previously been published, or given for the purpose of publication, by the individual.<sup>150</sup>

10.131 Under the draft Bill, a report of the commissioner must not make an adverse comment about a person unless the commissioner has given the person an opportunity to respond, in writing, to the proposed comment and any response from the person is fairly stated in the report. An 'adverse comment' does not include a statement that a person did not participate in resolving a complaint under the legislation.

<sup>145</sup> See *Information Privacy Act 2009* (Qld) s 193(2), (3); *Information Privacy Regulation 2009* (Qld) s 5(2); *Human Rights Act 2019* (Qld) s 91(1), (2)(e)–(j). See also, eg, VLRC Report No 18 (2010) Rec 4 at [10.48] above.

<sup>146</sup> As to '14' sitting days, cf *Health Ombudsman Act 2013* (Qld) s 169.

<sup>147</sup> Cf *Human Rights Act 2019* (Qld) ss 92(1)–(3), 94.

<sup>148</sup> See [10.113] above.

<sup>149</sup> See [10.113], [10.115] and [10.117] above.

<sup>150</sup> For this provision, 'personal information' has the same meaning as given in the *Information Privacy Act 2009* (Qld) s 12, namely:

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.

10.132 These safeguards are consistent with the approach taken under the *Human Rights Act 2019*, and will provide appropriate privacy and procedural fairness protections.<sup>151</sup>

### **Protections and offences**

10.133 Consistently with other legislation,<sup>152</sup> the draft Bill includes a small number other standard protective provisions and offences relating to the actions of and dealings with the commissioner, which are intended to ensure the effective operation of the commissioner's functions.

### ***Protections from civil liability***

10.134 The draft Bill protects the commissioner from civil liability for acts done or omissions made honestly and without negligence under the legislation.<sup>153</sup>

10.135 It also provides that, where a person, acting honestly, gives information or a written response to the commissioner under a provision of the legislation, the person is not liable (civilly, criminally or under an administrative process) because the person gave the information or response.<sup>154</sup> Neither can the person be held to have breached a code of professional etiquette or ethics or departed from accepted standards of professional conduct because the person gave the information or response.

10.136 This would apply, for example, where a person provides information to the commissioner in response to a notice under clause 76 of the draft Bill, or where a person provides a written response to a proposed adverse comment in a report of the commissioner under clause 87 of the draft Bill.<sup>155</sup>

### ***Confidentiality***

10.137 The draft Bill imposes a general obligation of confidentiality on persons performing functions under the legislation. A person who is or has been the commissioner or a staff member of the commission and who, in that capacity, acquires or has access to or custody of confidential information must not make a record of or disclose the information to another person.

10.138 'Confidential information means any information that:

- relates to a complaint made under the draft Bill;

<sup>151</sup> See *Human Rights Act 2019* (Qld) ss 91(4), 92(4), 93. See also, eg, *Ombudsman Act 2001* (Qld) s 55.

<sup>152</sup> See, eg, *Information Privacy Act 2009* (Qld) ss 153, 183, 186, 187, 188(a); *Right to Information Act 2009* (Qld) s 165; *Anti-Discrimination Act 1991* (Qld) ss 220, 221, 264, 265, 266; *Human Rights Act 2019* (Qld) ss 78(5)–(8), 99.

<sup>153</sup> Liability instead attaches to the State. As to the civil liability of a staff member of the commission, see *Public Service Act 2008* (Qld) ss 26B(4) and 26C.

<sup>154</sup> Under the draft Bill, 'information' is defined to include a record in any form and a document.

<sup>155</sup> See [10.105], [10.131] above.

- is personal information about a complainant, respondent or another individual;<sup>156</sup>
- is about a person's financial position or background; or
- if disclosed, would be likely to damage the commercial activities of a person to whom the information relates.

10.139 It does not, however, include information that is publicly available, or statistical or other information that is not likely to identify the person to whom it relates.

10.140 The obligation does not apply if the record is made or the information is disclosed with the consent of each person to whom the record or information relates, in performing a function under the legislation, or as required or permitted by another Act.

10.141 This general confidentiality provision applies subject to the specific provision the Commission recommends for the confidentiality of mediation<sup>157</sup> and to the following provision relating to the communication of official information to a court.<sup>158</sup>

10.142 The draft Bill includes a provision to the effect that a person who is or has been the commissioner, or a staff member of the commission, cannot be required to give information related to the performance of their functions under the legislation to a court. This provision does not apply if the information is given in performing a function under the legislation or as required or permitted by another Act.<sup>159</sup>

## Offences

10.143 The draft Bill includes a provision making it an offence for a person, in relation to the administration of the legislation, to give information to the commissioner or a staff member of the commission that the person knows is false or misleading in a material particular.

10.144 It is also an offence under the draft Bill for a person to fail, without reasonable excuse, to comply with a direction of the commissioner, given in a notice, requiring the person to give information to the commissioner.<sup>160</sup> It is a reasonable excuse for this provision if compliance would require disclosure of information that is

---

<sup>156</sup> For this provision, 'personal information' has the same meaning as given in the *Information Privacy Act 2009* (Qld) s 12: see n 150 above.

<sup>157</sup> See Rec 9-22 above.

<sup>158</sup> See [10.142] and Rec 10-18(d) below.

<sup>159</sup> Under the draft Bill, 'court' is defined for this provision to include any tribunal, authority or person having power to require the production of documents or the answering of questions; and 'give', to a court, is defined to include produce in the court and permit the court access to.

<sup>160</sup> See [10.105] above.

the subject of legal professional privilege, or information that might tend to incriminate the individual.<sup>161</sup>

10.145 The Commission considers it appropriate for these provisions—which concern a person’s failure to cooperate with the commissioner in the exercise of his or her functions—to be dealt with as offences. This will provide an enforcement mechanism and a disincentive to non-compliance. However, the Commission considers that a minor penalty is appropriate in this context. Accordingly the maximum penalty for these offences under the draft Bill is 10 penalty units.<sup>162</sup>

## Review of decisions

10.146 Decisions made by the commissioner will be subject to review under the *Judicial Review Act 1991*, in the same way as any other decision of an administrative character made under an enactment.<sup>163</sup>

## RECOMMENDATIONS

### A new independent regulator

**10-1 There should be an independent regulator. For the purpose of the draft Bill, the independent regulator is established as a separate entity under Recommendation 10-2 below. If the independent regulator’s functions were instead to be conferred on an existing entity, some of the recommended provisions would need appropriate modification. Whichever way the independent regulator is established, it should have the functions, powers and main features set out below.**

*[See Surveillance Devices Bill 2020 pt 5, and [10.64]–[10.88] above.]*

### Establishment of the regulator

**10-2 There should be a Surveillance Devices Commission (the ‘commission’). The commission:**

**(a) is a statutory body for the *Financial Accountability Act 2009* and the *Statutory Bodies Financial Arrangements Act 1982*; and**

<sup>161</sup> Express provision is included to make it clear that it is not intended by this offence to abrogate the privilege against self-incrimination. See generally Office of Queensland Parliamentary Counsel, ‘Self-incrimination’ in *Principles of Good Legislation: OQPC Guide to FLPs* (19 June 2013) [12].

<sup>162</sup> This also applies for the provision at [9.74], Rec 9-11 above.

Proceedings for these offences would be summary proceedings which may be commenced by a complaint in writing by the commissioner or a person authorised by the commissioner, within a limitation period of 12 months: see *Acts Interpretation Act 1954* (Qld) s 44(1), (2)(d), (4); *Justices Act 1886* (Qld) ss 42(1), 52(1).

<sup>163</sup> See generally *Judicial Review Act 1991* (Qld) ss 3 (definitions of ‘enactment’ and ‘reviewable matter’), 4(a), 5, 7, pt 3.

- (b) consists of the Surveillance Devices Commissioner appointed under Recommendation 10-3 below, and the staff of the commission employed under Recommendation 10-7 below.

*[See Surveillance Devices Bill 2020 cll 66, 67, and [10.89]–[10.90] above.]*

**10-3 The Surveillance Devices Commissioner (the ‘commissioner’):**

- (a) is appointed by, and holds office on the terms and conditions decided by, the Governor in Council;
- (b) holds office for a term of not more than five years stated in the instrument of appointment and, if a person is reappointed as commissioner, may hold office for not more than ten years continuously; and
- (c) controls the commission.

*[See Surveillance Devices Bill 2020 cll 71, 77, 78(1)–(3), and [10.91]–[10.92], [10.99] above.]*

**10-4 The draft Bill should also include standard provisions dealing with leave of absence as commissioner, vacancy in office, the grounds on which a person may be removed from office as commissioner, and the preservation of certain rights of public service employees. Other relevant provisions of general application in the *Acts Interpretation Act 1954* will also apply.**

*[See Surveillance Devices Bill 2020 cll 78(4), 79, 80, 81, 82, and [10.93]–[10.94] above.]*

**10-5 The draft Bill should ensure the independence of the commissioner by providing that:**

- (a) in performing the commissioner’s functions, the commissioner must act independently, impartially and in the public interest; and
- (b) the commissioner is not subject to direction by any person about how the commissioner performs the commissioner’s functions.

Under Recommendation 10-12(d), (e), (f) and 10-16(b) below, the Minister may, however, request advice, assistance or an examination, and may require a report, about particular matters.

*[See Surveillance Devices Bill 2020 cll 69 and 70, and [10.95]–[10.96] above.]*

- 10-6** The commissioner may delegate to an appropriately qualified staff member of the commission the commissioner's functions or powers under the legislation or another Act. Provisions of general application in the *Acts Interpretation Act 1954* will apply to the delegation.

*[See Surveillance Devices Bill 2020 cl 93, and [10.97]–[10.98] above.]*

- 10-7** Staff of the commission:

- (a) are employed under the *Public Service Act 2008*; and
- (b) are not subject to direction, other than from the commissioner or a person authorised by the commissioner, about how the commissioner's functions are to be performed.

*[See Surveillance Devices Bill 2020 cl 83, and [10.100]–[10.101] above.]*

#### **Functions and powers**

- 10-8** The draft Bill should provide the following in relation to the commissioner's general functions and powers:

- (a) The commissioner has the functions and powers given by the legislation;
- (b) The commissioner has power to do all things that are necessary or convenient to be done to perform the commissioner's functions under the legislation; and
- (c) If the commissioner believes on reasonable grounds that a person may have information relevant to a complaint being dealt with by the commissioner or to another function being performed by the commissioner, the commissioner may, by written notice, ask or direct the person to give the information to the commissioner within a reasonable period.

*[See Surveillance Devices Bill 2020 cll 68 and 76(1)–(4), and [10.104]–[10.106] above.]*

- 10-9** The commissioner's functions include receiving and dealing with complaints under Recommendations 9-1 to 9-29 above. There should be a clear administrative division, supported by formal policies and procedures, between the commissioner's complaints handling and mediation functions and the other functions of the commissioner.

*[See Surveillance Devices Bill 2020 cl 72, and [10.107]–[10.108] above.]*

**10-10 The commissioner's guidance functions include:**

- (a) promoting understanding of and compliance with the legislation, including the general obligations in Recommendation 8-2 above;
- (b) providing information and guidance about the operation of the legislation;
- (c) providing education and training about the legislation, including the general obligations in Recommendation 8-2 above and the lawful use of surveillance devices;
- (d) issuing guidelines about any matter related to the commissioner's functions, including guidelines on any of the following matters:
  - (i) how the legislation applies;
  - (ii) how an exception in Recommendation 5-12 to 5-18 or 6-5 to 6-7 above applies, including examples;
  - (iii) best practice for the use of surveillance devices, and the communication or publication of surveillance information, in a way that respects individuals' privacy; and
  - (iv) making, referring and dealing with complaints under Recommendation 9-1 above; and
- (e) giving information and reasonable help to complainants and respondents in relation to their complaints and the processes under the legislation.

*[See Surveillance Devices Bill 2020 cl 73(1), and [10.109]–[10.112] above.]*

**10-11 The draft Bill should additionally provide that the guidelines issued under Recommendation 10-10(d) above must be published on the commissioner's website.**

*[See Surveillance Devices Bill 2020 cl 73(2), and [10.110] above.]*

**10-12 The commissioner's research, advice and monitoring functions include:**

- (a) undertaking or commissioning research to monitor:
  - (i) whether the legislation is achieving its purpose;



- (ii) how surveillance devices and surveillance device technologies are used in civil society;
- (iii) developments in surveillance device technology;
- (b) identifying and commenting on any issues relating to the use of surveillance devices in civil society, and the communication or publication of surveillance information;
- (c) identifying and commenting on legislative and administrative changes that would improve the operation of the legislation;
- (d) on request of the Minister or on the commissioner's own initiative, advising the Minister about matters relevant to the operation and administration of the legislation;
- (e) on request of the Minister, assisting the Minister to review the legislation under Recommendation 11-2 below; and
- (f) on request of the Minister, examining other Acts and proposed legislation to determine whether they are, or would be, consistent with the purpose of the legislation and the general obligations in Recommendation 8-2 above.

*[See Surveillance Devices Bill 2020 cl 74, and [10.113]–[10.114] above.]*

**10-13** The commissioner's compliance monitoring functions include examining—on the commissioner's own initiative or otherwise—the practices of relevant entities, in relation to the following matters, to monitor whether the practices comply with the legislation:

- (a) how the entities use surveillance devices, and communicate or publish surveillance information;
- (b) the surveillance device, and communication or publication, technologies used by the entities; and
- (c) the programs, policies and procedures of the entities in relation to each of the matters in paragraphs (a) and (b).

*[See Surveillance Devices Bill 2020 cl 75(1), and [10.115]–[10.117] above.]*

**10-14** For the purpose of Recommendation 10-13 above:

- (a) 'relevant entity' means:
  - (i) a 'public entity' within the meaning of the *Human Rights Act 2019*;

- (ii) an entity with an annual turnover of more than \$5 million for the current or previous financial year;
  - (iii) an entity that regularly or routinely uses a surveillance device, or communicates or publishes surveillance information;
  - (iv) an entity that uses a surveillance device to monitor crowds in places that are open to or used by the public, whether or not on the payment of a fee; and
  - (v) another entity prescribed by regulation.
- (b) 'relevant entity' does not include an entity to the extent its practices relate to enforcing a law of the State, including, for example, the Queensland Police Service or the Crime and Corruption Commission.

*[See Surveillance Devices Bill 2020 cl 75(2), and [10.118]–[10.120] above.]*

#### **Reporting requirements**

**10-15** In addition to the annual financial reporting requirements that will apply under the *Financial Accountability Act 2009*, the draft Bill should provide that:

- (a) as soon as practicable after the end of each financial year, the commissioner must give the Minister an annual report about the operation of the legislation;
- (b) without limiting paragraph (a), the annual report must include information for the financial year about the following matters:
  - (i) the number of complaints made or referred to the commissioner;
  - (ii) the types of complaints made or referred to the commissioner, including:
    - (A) the categories of entities to which the complaints relate;
    - (B) the uses of surveillance devices to which the complaints relate;
    - (C) the provisions of Recommendation 8-2 ff above to which the complaints relate;

- (iii) the outcome of complaints made or referred to the commissioner, including:
  - (A) the number of complaints the commissioner refused to deal with, or to continue to deal with, and the grounds for refusing under Recommendations 9-12 and 9-13 above;
  - (B) the number and type of complaints referred to another entity under Recommendation 9-15 above;
  - (C) the number and type of complaints resolved by the commissioner by mediation under Recommendation 9-19 above;
  - (D) the number and type of complaints referred to QCAT under Recommendation 9-29 above;
- (iv) the outcome of complaints referred to QCAT;
- (v) another matter prescribed by regulation.
- (c) the Minister must table a copy of the annual report in the Legislative Assembly within 14 sitting days after receiving the report.

*[See Surveillance Devices Bill 2020 cl 84, and [10.123]–[10.126] above.]*

**10-16** The draft Bill should also provide that:

- (a) the commissioner may at any time prepare a report about a matter relevant to the performance of the commissioner's functions under the legislation and give the report to the Minister;
- (b) the commissioner must, if asked by the Minister, prepare a report about a matter mentioned in paragraph (a) and give the report to the Minister as soon as practicable after it is prepared; and
- (c) the Minister must table a copy of a report given to the Minister under paragraph (a) or (b) in the Legislative Assembly within 14 sitting days after receiving the report.

*[See Surveillance Devices Bill 2020 cl 85, and [10.123], [10.127]–[10.128] above.]*

**10-17** The draft Bill should also provide the following safeguards in relation to a report of the commissioner prepared under Recommendation 10-15 or 10-16 above:

- (a) the report must not include personal information about an individual unless the individual has previously published the information, or gave the information for the purpose of publication; and
- (b) the report must not make an adverse comment about a person unless the commissioner has given the person an opportunity to respond, in writing, to the proposed comment and any response from the person is fairly stated in the report.

For paragraph (a), ‘personal information’ has the same meaning as under the *Information Privacy Act 2009*, section 12.

For paragraph (b), ‘adverse comment’ does not include a statement that a person did not participate in resolving a complaint under the legislation.

*[See Surveillance Devices Bill 2020 cll 86 and 87, and [10.129]–[10.132] above.]*

#### **Protections and offences**

**10-18** The draft Bill should include the following protective provisions and offences relating to the actions of and dealings with the commissioner, to ensure the effective operation of the commissioner’s functions:

- (a) The commissioner is protected from civil liability for acts done or omissions made honestly and without negligence under the legislation.
- (b) Where a person, acting honestly, gives information or a written response to the commissioner under a provision of the legislation:
  - (i) the person is not liable (civilly, criminally or under an administrative process) because the person gave the information or written response; and
  - (ii) the person cannot be held to have breached a code of professional etiquette or ethics or departed from accepted standards of professional conduct because the person gave the information or written response.

- (c) A person who is or has been the commissioner or a staff member of the commission and who, in that capacity, acquires or has access to or custody of confidential information must not make a record of or disclose the information to another person. This does not apply if the record is made or the information is disclosed with the consent of each person to whom the record or information relates, in performing a function under the legislation, or as required or permitted under another Act. 'Confidential information' means any information that:

- (i) relates to a complaint made under the legislation;
- (i) is personal information about a complainant, respondent or another individual;
- (iii) is about a person's financial position or background; or
- (iv) if disclosed, would be likely to damage the commercial activities of a person to whom the information relates.

This does not include information that is publicly available or to statistical or other information that is not likely to identify the person to whom it relates.

- (d) A person who is or has been the commissioner, or a staff member of the commission, cannot be required to give information related to the performance of functions under the legislation to a court. This does not apply if the information is given in performing a function under the legislation, or as required or permitted by another Act.

- (e) It is an offence, with a maximum penalty of 10 penalty units:

- (i) for a person, in the administration of the legislation, to give information to the commissioner or a staff member of the commission that the person knows is false or misleading in a material particular; or
- (ii) for a person to fail, without reasonable excuse, to comply with a direction of the commissioner, given in a notice, requiring the person to give information to the commissioner. It is a reasonable excuse for this provision if compliance would require disclosure of information that is the subject of legal professional privilege, or information that might tend to incriminate the individual.

*[See Surveillance Devices Bill 2020 cll 76(5)–(6), 88, 89, 90, 91 and 92, sch 1 (definition of 'information') and [10.133] ff above.]*



# Chapter 11

## General matters

REGULATION-MAKING POWER .....	313
REVIEW OF ACT .....	313
CONSEQUENTIAL AMENDMENTS AND RELATED MATTERS .....	314
Acts referring to the <i>Invasion of Privacy Act 1971</i> .....	314
Statements relating to the use of an optical surveillance device .....	315
Sections 43(2)(c) and (e) and 45(2)(e) of the <i>Invasion of Privacy Act 1971</i> .....	316
RECOMMENDATIONS .....	317

### REGULATION-MAKING POWER

11.1 The draft Bill provides that the Governor in Council may make regulations under the legislation. This may include regulations to prescribe the fees payable under the legislation and to provide for a maximum penalty of 20 penalty units for a contravention of a regulation.

11.2 Other matters that might be the subject of regulations include:

- prescribing other circumstances in which a person who uses, installs or maintains a surveillance device does not commit an offence, pursuant to clause 26(b) of the draft Bill;
- prescribing other circumstances in which a person who communicates or publishes surveillance information does not commit an offence, pursuant to clause and 31(1)(f) of the draft Bill;
- prescribing another entity as a ‘relevant entity’ for the purposes of the commissioner’s compliance monitoring functions, pursuant to clause 75(2)(a)(v) of the draft Bill; or
- prescribing another matter that must be included in the commissioner’s annual report, pursuant to clause 84(2)(e) of the draft Bill.

### REVIEW OF ACT

11.3 The draft Bill provides that the Minister must complete a review of the effectiveness of the legislation within five years after its commencement. The Commission considers that this requirement is appropriate, given the scope and application of the new legislative framework for regulating the use of surveillance devices.

11.4 In completing the review, the Minister must consider whether the legislation is achieving its purpose, developments in surveillance device technology, how surveillance devices and surveillance device technologies are used in civil society,

and whether the legislation should be amended to provide for new types of surveillance devices or new uses of surveillance devices and surveillance device technologies in civil society.

11.5 The draft Bill also provides that the Minister must table a report on the outcome of the review in the Legislative Assembly as soon as practicable after the review is completed.

## CONSEQUENTIAL AMENDMENTS AND RELATED MATTERS

11.6 The Commission recommends that the *Invasion of Privacy Act 1971* be repealed and replaced by new legislation regulating the use of surveillance devices, in the form of the draft Bill.<sup>1</sup> There are a number of Queensland Acts that will, or may, require consequential amendments if legislation based on the draft Bill is enacted.

### Acts referring to the *Invasion of Privacy Act 1971*

11.7 There are several Acts that include references to the *Invasion of Privacy Act 1971* for the purposes of the following provisions of those Acts:

- Section 19C of the *Commissions of Inquiry Act 1950*, which empowers a Supreme Court judge, on the application of a chairperson of a commission of inquiry, to approve the use of a listening device (within the meaning of the *Invasion of Privacy Act 1971*) to obtain information relevant to the commission's inquiry with respect to any offence;<sup>2</sup>
- Section 181A of the *Fisheries Act 1994*, which provides that it is lawful for an inspector to use a body-worn camera to record images or sounds while the inspector is exercising powers under Part 8 of the Act;
- Section 609A of the PPRA, which provides that it is lawful for a police officer to use a body-worn camera to record images or sounds while the officer is acting in the performance of the officer's duties;
- Section 43E of the *Public Safety Preservation Act 1986*, which empowers a commissioned officer, during an emergency, to authorise a police officer to use a surveillance device in an emergency area and during the period of the emergency to assess and monitor a serious risk to the life, health or safety of a person (a 'surveillance device authorisation'); and
- Section 263A of the *Youth Justice Act 1992*, which empowers the chief executive of the Department of Youth Justice to record images or sounds in a detention centre, or to authorise a detention centre employee to use a body-worn camera to record images or sounds while the employee is acting in the performance of the employee's duties.

<sup>1</sup> See [3.10], Rec 3-1 above.

<sup>2</sup> Relevantly, the *Commissions of Inquiry Act 1950* (Qld) adopts the definition of 'listening device' in s 4 of the *Invasion of Privacy Act 1971* (Qld): *Commissions of Inquiry Act 1950* (Qld) s 3 (definition of 'listening device').



11.8 Each of those provisions is a provision of an Act authorising the use of a listening device, and therefore falls within the exception in section 43(2)(d) of the *Invasion of Privacy Act 1971* to the prohibition on the use of a listening device or in section 45(2)(e) to the prohibition on the communication or publication of a private conversation by a party to the conversation.<sup>3</sup>

11.9 Each reference to the *Invasion of Privacy Act 1971* is made in a particular context, for example, in the context of a provision that: states that the relevant authorising provision is a provision authorising the use of a listening device for the purposes of section 43(2)(d) of the *Invasion of Privacy Act 1971*;<sup>4</sup> applies the definition of 'listening device' in the *Invasion of Privacy Act 1971* for the purposes of the relevant authorising provision;<sup>5</sup> or declares how the relevant authorising provision affects the operation of other laws relating to the use of listening devices or other surveillance devices.<sup>6</sup>

11.10 As a result of the repeal of the *Invasion of Privacy Act 1971*, each of those Acts will require consequential amendment to omit the references to the *Invasion of Privacy Act 1971*, and to insert references to the legislation in their place, as appropriate.

11.11 Consideration will be also required as to whether, as a matter of policy, the references in those Acts to a 'listening device' (or, where relevant, to the prohibition against the use of a listening device) should be amended to also refer to other categories of surveillance devices regulated under the draft Bill, as appropriate.<sup>7</sup> This may require a consideration of policy matters specific to the Act being amended.

### Statements relating to the use of an optical surveillance device

11.12 Chapter 13 of the PPRA establishes procedures for law enforcement officers to obtain a warrant or emergency authorisation for the installation, use, maintenance and retrieval of surveillance devices in particular criminal investigations.<sup>8</sup> Section 325 of the PPRA deals with the relationship between Chapter 13 and other laws and matters. Section 325(7) is a declaratory provision which provides that:

<sup>3</sup> See *Commissions of Inquiry Act 1950* (Qld) s 19C(1), (3); *Fisheries Act 1994* (Qld) s 181A(1); *Police Powers and Responsibilities Act 2000* (Qld) s 609A(1); *Public Safety Preservation Act 1986* (Qld) s 43E(1)–(6); *Youth Justice Act 1992* (Qld) s 263A(1), (2), (6).

<sup>4</sup> See *Fisheries Act 1994* (Qld) s 181A(4), *Police Powers and Responsibilities Act 2000* (Qld) s 609A(4); *Youth Justice Act 1992* (Qld) s 263A(7).

<sup>5</sup> See *Commissions of Inquiry Act 1950* (Qld) s 3 (definition of 'listening device'); *Youth Justice Act 1992* (Qld) s 263A(8) (definition of 'listening device').

<sup>6</sup> See *Public Safety Preservation Act 1986* (Qld) s 43E(7).

<sup>7</sup> For example, a body-worn camera that records images or sounds would fall within the definitions of 'listening device' and 'optical surveillance device' under the draft Bill: see [4.57]–[4.60] above.

<sup>8</sup> For the purposes of ch 13 of that Act, a 'surveillance device' is a data surveillance device, a listening device, an optical surveillance device or a tracking device or a device that is a combination of any two or more of those devices: *Police Powers and Responsibilities Act 2000* (Qld) s 322 (definition of 'surveillance device'). The definitions of 'data surveillance device', 'listening device', 'optical surveillance device' and 'tracking device' that apply for ch 13 of that Act are similar to those that apply under the draft Bill, subject to minor variations: see *Police Powers and Responsibilities Act 2000* (Qld) s 322 (definitions of 'data surveillance device', 'listening device', 'optical surveillance device' and 'tracking device').

[Chapter 13] does not stop a law enforcement officer from using an optical surveillance device in a place where the presence of the police officer is not an offence.

*Examples—*

- 1 The police officer may use an optical surveillance device to record activities in a public place or, with the occupier's consent, install the device in a private place.
- 2 A police officer who is lawfully at a place may use binoculars or a telescope to monitor activities at a place the police officer is not lawfully entitled to enter.

11.13 A similar provision is included in section 43E of the *Public Safety Preservation Act 1986*, which provides for the authorisation of a police officer to use a surveillance device in emergency circumstances.<sup>9</sup> Section 43E(7) of the *Public Safety Preservation Act 1986* provides that section 43E does not stop a police officer from:

- using an optical surveillance device in a place where the presence of the police officer is not an offence; or
- using a listening device, in a place where the presence of the police officer is not an offence, to overhear, record, monitor or listen to a conversation, if the use is not an offence against s 43(1) of the *Invasion of Privacy Act 1971*.

11.14 If legislation based on the draft Bill is enacted, section 325(7) of the PPRA (and the examples of how that provision operates) and section 43E(7) of the *Public Safety Preservation Act 1986* should be reviewed in light of the criminal provisions in the draft Bill prohibiting the use of optical surveillance devices (which make it an offence to observe, monitor or visually record a private activity without the consent of each party to the activity, unless an exception applies), and other categories of surveillance devices regulated by the draft Bill, as appropriate.

### **Sections 43(2)(c) and (e) and 45(2)(e) of the *Invasion of Privacy Act 1971***

11.15 Section 43(2)(c) and (e) of the *Invasion of Privacy Act 1971* provides specific exceptions to the prohibition on the use of a listening device in section 43(1) of that Act. These exceptions are limited in their application to or in relation to the use of a listening device:

- by an officer employed in the service of the Commonwealth in relation to customs authorised by a warrant issued by the Comptroller-General of Customs under the *Customs Act 1901* (Cth) to use a listening device in the performance of the officer's duty (section 43(2)(c)(i));
- by a person employed in connection with the security of the Commonwealth when acting in the performance of the person's duty under a Commonwealth Act relating to the security of the Commonwealth (section 43(2)(c)(ii)); and

---

<sup>9</sup> See [11.7] above.

- that is a government network radio, activated by a communications centre operator for a public safety entity, in circumstances in which—
  - an officer of the entity has activated a duress alarm; or
  - an officer of the entity has contacted the communications centre operator to ask for assistance; or
  - the communications centre operator has reasonable grounds to believe there may be a risk to the life, health or safety of an officer of the entity (section 43(2)(e)).<sup>10</sup>

11.16 Section 45(2)(e) of the *Invasion of Privacy Act 1971* provides an exception to the prohibition on communication or publication of a private conversation by a party to the conversation. It applies where the communication or publication is made by a person who used a listening device pursuant to the exceptions in mentioned in section 43(2)(c) and (d) above.

11.17 The regulation of the use of surveillance devices under the draft Bill is based on different principles and policy settings from the *Invasion of Privacy Act 1971*. In particular, the draft Bill includes prohibitions on the use of a surveillance device and the communication or publication of information obtained from the use of a surveillance device, as well as a number of general purpose-based exceptions to the those prohibitions.<sup>11</sup> The Commission has not made recommendations in relation to section 43(2)(c) and (e) and section 45(2)(e) given that they relate to matters of government policy and operate in a specific context. Those provisions should be reviewed in light of the approach taken in the draft Bill and the specific policy matters relevant to them.

## RECOMMENDATIONS

### Regulation-making power

**11-1 The draft Bill should provide that the Governor in Council may make regulations under the legislation.**

*[See Surveillance Devices Bill 2020 cl 94 and [11.1]–[11.2] above.]*

<sup>10</sup>

Section 43(7) of the *Invasion of Privacy Act 1971* (Qld) defines: a 'communications centre operator', for a public safety entity, to mean a person who is employed or otherwise engaged by the entity, whether on a paid or voluntary basis, to maintain radio contact with officers of the entity; a 'government network radio' to mean a radio that uses a secure digital radio communications network to enable a communications centre operator for a public safety entity and an officer of the entity to communicate with each other, and that may be fitted to a vehicle or carried by a person; an 'officer', of a public safety entity, to mean a person who is employed or otherwise engaged by the entity, whether on a paid or voluntary basis; and a 'public safety entity' to mean the Queensland Ambulance Service established under the *Ambulance Service Act 1991* (Qld), the Queensland Police Service, or any of the following entities established under the *Fire and Emergency Services Act 1990* (Qld)—the Queensland Fire and Emergency Service, the State Emergency Service, an emergency service unit, or a rural fire brigade registered under the *Fire and Emergency Services Act 1990* (Qld).

<sup>11</sup>

See, Chapters 5 and 6 above, respectively, as to the use prohibitions and communication or publication prohibitions and their respective exceptions.

**Review of Act**

**11-2** The draft Bill should provide that the Minister must complete a review of the effectiveness of the legislation within five years after the commencement. In completing the review, the Minister must consider:

- (a) whether the legislation is achieving its purpose; and
- (b) how surveillance devices and surveillance device technologies are used in civil society; and
- (c) developments in surveillance device technology; and
- (d) whether the legislation should be amended to provide for:
  - (i) new types of surveillance devices; or
  - (ii) new uses of surveillance devices and surveillance device technologies in civil society.

In addition, the Minister must table in the Legislative Assembly a report on the outcome of the review as soon as practicable after the review is completed.

*[See Surveillance Devices Bill 2020 cl 95 and [11.3] ff above.]*

**Consequential provisions**

**11-3** If legislation based on the draft Bill is enacted, the references to the '*Invasion of Privacy Act 1971*' in the following Acts should be omitted and replaced by references to the legislation, as appropriate:

- (a) the *Commissions of Inquiry Act 1950*;
- (b) the *Fisheries Act 1994*;
- (c) the *Police Powers and Responsibilities Act 2000*;
- (d) the *Public Safety Preservation Act 1986*; and
- (e) the *Youth Justice Act 1992*.

*[See [11.7] ff above]*

# 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.<sup>1</sup>

### 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~~ 28 February 2020.<sup>2</sup>

Dated the 24th day of July 2018

**YVETTE D'ATH MP**

Attorney-General and Minister for Justice  
Leader of the House

---

<sup>1</sup> On 7 December 2018, the Attorney-General and Minister for Justice, Leader of the House, the Hon Yvette D'Ath MP, by letter, amended the terms of reference, at the Commission's request, to ask the Commission to prepare draft legislation based on its recommendations.

<sup>2</sup> On 7 December 2018, the Attorney-General and Minister for Justice, Leader of the House, the Hon Yvette D'Ath MP, by letter, amended the terms of reference to extend the reporting date from 1 July 2019 to 31 October 2019. On 3 October 2019, the Attorney-General and Minister for Justice, Leader of the House, the Hon Yvette D'Ath MP, by letter, amended the terms of reference to extend the reporting date from 31 October 2019 to 28 February 2020.





## Appendix B

### List of respondents

1	Peter Biglands
2	Joshua Allan
3	Name withheld from publication
4	Bill Tait (Jnr)
5	Jennifer Redmond
6	Name withheld from publication
7	Justin Cobbett
8	NSW Privacy Commissioner
9	Mental Health Review Tribunal
10	Department of Education
11	Krysten
12	Dr Wayne Bovey
13	Rose Bovey
14	Professor Rick Sarre
15	Department of Agriculture and Fisheries
16	Department of Environment and Science
17	Dr Jeremy Patrick
18	Toowoomba Regional Council
19	Professor Des Butler
20	Confidential
21	Queensland Nurses and Midwives' Union ('QNMU')
22	Denise
23	Council of the City of Gold Coast
24	Department of State Development, Manufacturing, Infrastructure and Planning ('DSDMIP')
25	Future Wise
26	Insurance Council of Australia
27	Women's Legal Service Qld

28	Spatial Industries Business Association Geospatial Information Technologies Association (Australia, New Zealand)
29	David Cosgrave
30	His Honour Judge Orazio Rinaudo AM, Chief Magistrate
31	Queensland Treasury
32	Queensland Government Chief Information Office, Department of Housing and Public Works ('QGCIIO')
33	Queensland Advocacy Incorporated ('QAI')
34	Confidential
35	Brisbane City Council
36	Department of Transport and Main Roads
37	Animal Liberation Queensland
38	Office of the Information Commissioner (Queensland) ('OIC')
39	Australian Association for Unmanned Systems ('AAUS')
40	Queensland Council for Civil Liberties
41	Townsville Community Legal Service Inc.
42	Confidential
43	Queensland Law Society ('QLS')
44	Tandida Mea
45	Confidential
46	Kellie Anderson
47	Megan Pictor

# Appendix C

## Comparative guide to surveillance devices legislation

[C.1] Table 1 is a brief comparison between the main provisions of the surveillance devices legislation in each Australian jurisdiction,<sup>1</sup> and those the Commission recommends in the draft Bill.

[C.2] This is supplemented by Tables 2 and 3, which outline the exceptions to the criminal offences relating to the use of a surveillance device, and the communication or publication of information obtained from the use of a surveillance device, respectively.

[C.3] In these tables, the following abbreviations are used for each category of surveillance device:

- L—listening device;
- O—optical surveillance device;
- T—tracking device;
- D—data surveillance device.

[C.4] The tables should be read together with the discussion in the body of the Report.

---

<sup>1</sup> *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). Tables 1, 2 and 3 do not include information about criminal offences, or exceptions to criminal offences, that apply to law enforcement officers only.

**TABLE 1: Comparative table of surveillance devices legislation**

		ACT	NSW	NT	SA	TAS
Regulation of surveillance devices	Recognised categories of surveillance devices	L	L, O, T, D	L, O, T <sup>2</sup>	L, O, T, D	L
	Scope to add new devices		✓ (by regulation)	✓ (by regulation)	✓ (by regulation)	
Criminal offences <sup>3</sup>	Use of a surveillance device	✓	✓ (without consent for O, T, D)	✓ (without consent)	✓ (without consent for O, T, D)	✓
	Communication or publication of surveillance information	✓ (obtained by a party, by unlawful use, or by use pursuant to some exceptions; private conversation)	✓ (obtained through unlawful use; private conversation or carrying on of activity, or information about a computer)	✓ (private conversation or private activity)	✓ (obtained by unlawful use)	✓ (obtained by a party, or by unlawful or unintentional use; private conversation)
Exceptions	Participant monitoring <sup>4</sup>			✓		
	There are various exceptions to the criminal offences relating to the use of a surveillance device, or the communication or publication of surveillance information. These exceptions differ between jurisdictions. They include, for example, use, communication or publication to protect a person's lawful interest, in the public interest or for a person's safety and well-being. See Tables 2 and 3.					
Ancillary matters	Offence of possession of surveillance information <sup>5</sup>	✓ (obtained by unlawful use; private conversation)	✓ (obtained by unlawful use; private conversation or carrying on of activity)			✓ (obtained by unlawful or unintentional use; private conversation)
	Restriction on admissibility of evidence obtained by unlawful use of surveillance device	✓				✓
	Non-publication orders	✓				✓
	Forfeiture orders (surveillance device and surveillance information)	✓	✓	✓	✓	✓

<sup>2</sup> Legislation in the Northern Territory and Victoria regulates the use of a data surveillance device, and the communication or publication of information obtained from their use, by law enforcement officers and, in the Northern Territory, by an Independent Commission Against Corruption officer only: *Surveillance Devices Act* (NT) ss 14, 16; *Surveillance Devices Act 1999* (Vic) ss 9, 12. Those provisions are not included here.

<sup>3</sup> For an overview of the criminal offences in each jurisdiction, see [2.20] ff above and QLRC Consultation Paper No 77 (2018) [3.50], [3.167]. As to consent, see also Tables 2 and 3, which address consent as an exception to the offences.

<sup>4</sup> Participant monitoring is permitted in Queensland, the Northern Territory and Victoria. The prohibition on the use of an optical surveillance device in New South Wales may permit participant monitoring: see [5.245] and n 226 above.

<sup>5</sup> However, except in Western Australia, a person will not commit an offence if a record is in their possession in connection with proceedings for an offence, with consent, or as a consequence of a communication or publication of that record to that person in a way that does not contravene the draft Bill: see [7.3] ff above.

In Queensland and some other jurisdictions, it is also an offence to possess, manufacture, supply or advertise a surveillance device, or to unlawfully enter a dwelling house. Those offences are not included in the draft Bill: see [7.9] ff and [7.47] ff above.

VIC	WA	QLD	QLRC Draft Bill		
L, O, T <sup>2</sup>	L, O, T	L	L, O, T, D	Recognised categories of surveillance devices	Regulation of surveillance devices
✓ (by regulation)			✓ (provision for review of Act)	Scope to add new devices	
✓ (without consent)	✓ (without consent for T)	✓	✓ (without consent)	Use of a surveillance device	Criminal offences <sup>3</sup>
✓ (private conversation or private activity)	✓ (private conversation or private activity)	✓ (obtained by a party, or by unlawful use; private conversation)	✓ (without consent; private conversation or private activity, geographical location or information about a computer)	Communication or publication of surveillance information	
✓		✓		Participant monitoring <sup>4</sup>	
There are various exceptions to the criminal offences relating to the use of a surveillance device, or the communication or publication of surveillance information. These exceptions differ between jurisdictions. They include, for example, use, communication or publication to protect a person's lawful interest, in the public interest or for a person's safety and well-being. See Tables 2 and 3.					Exceptions
	✓		✓ (obtained by unlawful use; private conversation or private activity, geographical location or information about a computer)	Offence of possession of surveillance information <sup>5</sup>	Ancillary matters
		✓		Restriction on admissibility of evidence obtained by unlawful use of surveillance device	
		✓	✓	Non-publication orders	
	✓	✓ (device only)	✓	Forfeiture orders (surveillance device and surveillance information)	

		ACT	NSW	NT	SA	TAS
Civil law obligations	General obligations not to use a surveillance device, or communicate or publish surveillance information, in a way that interferes with an individual's surveillance privacy					
	A person will not contravene the general obligations in the draft Bill if the individual has consented to the use, communication or publication, or if the person did not know, and ought not reasonably to have known, that the use, communication or publication would interfere with the individual's surveillance privacy. In addition, there are exceptions to the general obligations, namely where the use, communication or publication is: authorised or required by law or by an order or process of a court or tribunal; incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property; or reasonably necessary in the public interest.					
Complaints process	Complaints about alleged contraventions of the general obligations		(NSWLRC: NSW Privacy Commissioner should have additional functions to investigate and conciliate complaints, and if unresolved refer to Administrative Decisions Tribunal)			
	Civil remedies <sup>6</sup>		(NSWLRC: Administrative Decisions Tribunal should have power to grant relief, including damages up to \$150 000)			
Independent regulator	Regulator with functions under surveillance devices legislation		(NSWLRC: NSW Privacy Commissioner should have additional functions regarding overt surveillance)			

6

The ALRC recommended that surveillance devices legislation should follow the approach of the *Telecommunications (Interception and Access) Act 1979* (Cth). Those provisions empower a court, when a relevant offence prohibition is contravened, to make appropriate orders against the defendant, including an order for damages: see [9.21] ff above.

VIC	WA	QLD	QLRC Draft Bill		
			✓	General obligations not to use a surveillance device, or communicate or publish surveillance information, in a way that interferes with an individual's surveillance privacy	Civil law obligations
A person will not contravene the general obligations in the draft Bill if the individual has consented to the use, communication or publication, or if the person did not know, and ought not reasonably to have known, that the use, communication or publication would interfere with the individual's surveillance privacy. In addition, there are exceptions to the general obligations, namely where the use, communication or publication is: authorised or required by law or by an order or process of a court or tribunal, incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property; or reasonably necessary in the public interest.					
(VLRC: Victorian Privacy Commissioner should have additional functions to investigate and take civil proceedings about breaches of legislation)			✓ (mediated or, if not resolved, referred to QCAT for decision)	Complaints about alleged contraventions of the general obligations	Complaints process
			✓ (civil orders for complaints referred to QCAT, including compensation up to \$100 000)	Civil remedies <sup>6</sup>	
(VLRC: Victorian Privacy Commissioner should have additional functions to guide the responsible use of surveillance in public places)			✓ (functions include guidance, education, research and monitoring)	Regulator with functions under surveillance devices legislation	Independent regulator

TABLE 2: Use exceptions

	Qld (L)	ACT (L)	NSW (L, O, T, D)	NT (L, O, T)	SA (L, O, T, D)	Tas (L)	Vic (L, O, T)	WA (L, O, T)	Draft Bill (L, O, T, D)
By a party, with consent of all principal parties to a private conversation or private activity <sup>7</sup>		✓ (L)	✓ (L)		✓ (L)	✓ (L)		✓ (L, O)	
By a party, with consent of a principal party, to protect lawful interests of that principal party		✓ (L)	✓ (L)		✓ (L, by party to protect their lawful interests)	✓ (L)		✓ (L, O)	
By a person, to protect lawful interests of person					✓ (L, on premises or vehicle with consent; O, on premises for user's lawful interests)				✓ (L, O, T, D)
By a party, with consent of principal party, not for communication or publication to a non-party		✓ (L)	✓ (L)			✓ (L)			
In the public interest (Use that is either general or specific, eg, with consent of a party, to protect a vulnerable person who is a party, in an emergency)				✓ (L, O; emergency use only)	✓ (L, O)			✓ (L, O)	✓ (L, O, T, D)
In connection with safety and well-being (eg in connection with an imminent threat of violence or damage, or in relation to a vulnerable person) <sup>8</sup>				✓ (T)		✓ (L)		✓ (L, O, T)	✓ (L, O, T, D)
By private investigators and loss adjusters (Includes use for a lawful interest or in the public interest)					✓ (L, O)				
For the purpose of location and/or retrieval (Includes use to locate a device, or a vehicle or object that is lost or stolen)			✓ (L, O)		✓ (L, O, T)			✓ (T, stolen)	✓ (L, O, T, D)
For a lawful purpose			✓ (T)						
Unintentional use (Includes unintentional hearing, and sometimes unintentional recording)	✓ (L, hear by phone)	✓ (L)	✓ (L)		✓ (L)	✓ (L)		✓ (L, O)	
In prescribed circumstances <sup>9</sup>				✓ (T)	✓ (L, O, T, D)			✓ (T)	✓ (L, O, T, D)
Authorised under an Act or law	✓ (L)	✓ (L)	✓ (L, O, T, D)	✓ (L, O, T)	✓ (L, O, T, D)	✓ (L)	✓ (L, O, T)	✓ (L, O, T)	✓ (L, O, T, D)

<sup>7</sup> In some jurisdictions, and in the draft Bill, consent is an element of the criminal offences, rather than an exception to those offences. In Queensland, the Northern Territory and Victoria, where participant monitoring is permitted, there are fewer circumstances in which consent is required: see Table 1 above.

Generally, a 'party' is a person by or to whom words are spoken during a private conversation, or a person taking part in a private activity. In Queensland, the Australian Capital Territory, New South Wales, Tasmania and Western Australia, a 'party' also includes a person who listens to, observes, monitors or records a conversation or an activity with consent: see [5.196]–[5.197] above.

<sup>8</sup> Except in relation to the draft Bill, where this exception applies to a tracking device, the exception appears in the regulations as a prescribed circumstance in which the use of a tracking device is not an offence.

<sup>9</sup> In each of the relevant jurisdictions, circumstances have been prescribed in relation to the use of a tracking device. In South Australia, no circumstances have been prescribed in relation to the use of a listening device, an optical surveillance device or a data surveillance device: see [5.347]–[5.348] above.



**TABLE 3: Communication or publication exceptions**

	Qld (L)	ACT (L)	NSW (L, O, T, D)	NT (L, O, T)	SA (L, O, T, D)	Tas (L)	Vic (L, O, T)	WA (L, O, T) <sup>10</sup>	Draft Bill (L, O, T, D)
<b>With consent of each principal party to a private conversation or private activity<sup>11</sup></b>	✓ (L, for a person, with consent of a party)	✓ (L)	✓ (L, O, T)	✓ (L, O, T)	✓ (L, O, T, D; with consent of each party)	✓ (L)	✓ (L, O, T)	✓ (L, O)	✓ (L, O, T, D; prohibited without consent)
<b>To a party to a private conversation or activity</b>	✓ (L)	✓ (L)	✓ (L, O, T)		✓ (L, O, T, D)	✓ (L)		✓ (L, O)	
<b>To, or with consent of, person in lawful possession or control of computer</b>			✓ (D)						
<b>By a party, to protect lawful interests of that party</b>	✓ (L)	✓ (L)				✓ (L)			
<b>By a person to protect lawful interests of a principal party, where device used with consent of a principal party to protect their lawful interests</b>		✓ (L)						✓ (L, O)	
<b>By a person, to protect lawful interests of that person</b>				✓ (L, O, T)	✓ (L, O) <sup>12</sup>		✓ (L, O, T)	✓ (L, O)	✓ (L, O, T, D; or another person)
<b>In the public interest</b>	✓ (L, by a party)			✓ (L, O, T; with court order if L or O used in emergency)	✓ (L, O; with court order, but see media exception below)		✓ (L, O, T)	✓ (L, O; with court order)	✓ (L, O, T, D)
<b>In connection with safety and well-being</b> (eg in connection with an imminent threat of violence or damage, or some offences)			✓ (L, O, T, D)		✓ (L, O) <sup>12</sup>	✓ (L)		✓ (L, O)	✓ (L, O, T, D)
<b>To or by a media organisation</b> (eg where device used in the public interest to protect a lawful interest)					✓ (L, O)				
<b>In the performance of a duty</b>	✓ (L, by a party)				✓ (L, O, T, D)			✓ (L, O)	
<b>By a party, to a person with a reasonable interest in a private conversation</b>	✓ (L)	✓ (L)				✓ (L)			
<b>Where knowledge is obtained other than by unlawful use</b>	✓ (L)	✓ (L)	✓ (L, O, T, D)		✓ (L, O, T, D)	✓ (L)			
<b>In some or all legal proceedings<sup>13</sup></b>	✓ (L)	✓ (L)	✓ (L, O, T, D)	✓ (L, O, T)	✓ (L, O, T, D)	✓ (L)	✓ (L, O, T)	✓ (L, O)	✓ (L, O, T, D)

<sup>10</sup> In Western Australia, it is a general requirement of any exception to the communication or publication prohibitions that, among other things, 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; or 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 private activity as to make the communication or publication reasonable in the circumstances: *Surveillance Devices Act 1998* (WA) s 9(3)(a)–(b). See also, as to authorised use or use by an authorised person, s 9(3)(c)–(d).

<sup>11</sup> Generally, a ‘party’ is a person by or to whom words are spoken during a private conversation, or a person taking part in a private activity. In Queensland, the Australian Capital Territory, New South Wales, Tasmania and Western Australia, a ‘party’ also includes a person who listens to, observes, monitors or records a conversation or an activity with consent: see [5.196]–[5.197] above.

<sup>12</sup> In South Australia, where a person uses a listening device or an optical surveillance device to protect their lawful interests, communication or publication of information is not an offence in some circumstances, for example, where it is with consent, to a media organisation or with a court order. Also, it is not an offence where a person is being subjected to violence or there is an imminent threat of violence to a person: see [6.87] above.

<sup>13</sup> In New South Wales and South Australia, there is also an exception for communication or publication for the purpose of investigating or prosecuting an offence against the Act: see [6.78], n 75 in Chapter 6 above.

**TABLE 3: Communication or publication exceptions**

	Qld (L)	ACT (L)	NSW (L, O, T, D)	NT (L, O, T)	SA (L, O, T, D)	Tas (L)	Vic (L, O, T)	WA (L, O, T) <sup>10</sup>	Draft Bill (L, O, T, D)
In prescribed circumstances					✓ (L, O; licensed investigation agents and loss adjusters) <sup>14</sup>				✓ (L, O, T, D)
By a person who is authorised to use a surveillance device	✓ (L)								✓ (L, O, T, D)
By or to an authorised or specified person				✓ (L, O, T)			✓ (L, O, T)	✓ (L, O)	
Authorised under an Act or law		✓ (L)		✓ (L, O, T)	✓ (L, O, T, D)	✓ (L)	✓ (L, O, T)		✓ (L, O, T, D)
By a person, where a surveillance device was used unlawfully but knowledge was also obtained in some other way	✓ (L)	✓ (L)	✓ (L, O, T, D)		✓ (L, O, T, D)	✓ (L)			

14

As to the prescribed persons, classes of persons or circumstances for a licensed investigation agent, see *Surveillance Devices Regulations 2017* (SA) s 12 and [6.125] above. There are no persons or circumstances prescribed in relation to loss adjusters.

# Appendix D

## Other laws relevant to surveillance and privacy

[D.1] 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

[D.2] Under the Australian Constitution, the Commonwealth has the power to make laws with respect to ‘postal, telegraphic, telephonic and other like services’.<sup>1</sup> The Commonwealth has enacted the *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Telecommunications Act 1997* (Cth). Both Acts recognise and protect the privacy of individuals who communicate through the Australian telecommunications network.<sup>2</sup>

[D.3] The High Court has held that the *Telecommunications (Interception and Access) Act 1979* (Cth) exclusively regulates the interception of telephone communications,<sup>3</sup> 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.<sup>4</sup>

### Interception of telecommunications

[D.4] 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. The offence also applies if a person authorises, suffers or permits another person to intercept such a communication, or to do any act or thing that will enable the person or another person to intercept such a communication.<sup>5</sup>

---

<sup>1</sup> *Australian Constitution* s 51(v).

<sup>2</sup> *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; B Lloyd, J Von Thien and P Ward, ‘Interception of and access to communications’, *Communications Law and Policy in Australia* (2019) [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, *Lawful access to telecommunications: Telecommunications interception and surveillance* (30 January 2020) <<https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance>>.

<sup>3</sup> *Miller v Miller* (1978) 141 CLR 269, 276.

<sup>4</sup> See VLRC Report No 18 (2010) [1.22].

<sup>5</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) ss 6(1), 7(1), 105(1)–(2). The offence has a maximum penalty of two years imprisonment.

[D.5] 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 making the communication.<sup>6</sup> 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 a text message being sent and being delivered to the recipient's telephone provider.<sup>7</sup>

[D.6] 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.<sup>8</sup> Some common examples of a 'communication' are a telephone conversation, a text message or an email.<sup>9</sup> Communications solely by means of radiocommunication, such as bluetooth or walkie-talkie communications, are not included.<sup>10</sup>

[D.7] Effectively, the prohibition against interception is limited to 'live' or 'real-time' communications.<sup>11</sup> Once a communication is no longer being transmitted, a person

<sup>6</sup> *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 2, 194.

<sup>7</sup> 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.

<sup>8</sup> See Vanhear, above n 2, 194; Electronic Frontiers Australia, *Telecommunications (Interception and Access) Act 1979 (TIA)* <<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].

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).

<sup>9</sup> 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).

<sup>10</sup> *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].

<sup>11</sup> See Electronic Frontiers Australia, *Telecommunications (Interception and Access) Act 1979 (TIA)* (2018) <<https://www.efa.org.au/privacy/tia-new/>>.

is not prohibited by the *Telecommunications (Interception and Access) Act 1979* (Cth) from recording the conversation.<sup>12</sup> One commentator explains that:<sup>13</sup>

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)

[D.8] 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.<sup>14</sup>

### **Accessing stored communications**

[D.9] Stored communications, being communications that are not in transit and that have been held by a 'carrier' of communications services, are also protected.<sup>15</sup> Common examples of stored communications are emails, text messages and voice mail messages that are not in transit.<sup>16</sup>

[D.10] 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.<sup>17</sup>

<sup>12</sup> 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.

<sup>13</sup> Vanhear, above n 2, 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; Lloyd, Von Thien and Ward, above n 2, [610,800]; VLRC Report No 18 (2010) [1.22]; NSWLRC Report No 108 (2005) [2.4].

<sup>14</sup> *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.

<sup>15</sup> *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 9 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'), 26–29, 41, 56, 87.

<sup>16</sup> 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.

<sup>17</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(1)(a). The offence has a maximum penalty of two years imprisonment or 120 penalty units (\$25 200) or both.

The offence applies if the access (or other act or thing) is done without the knowledge of the intended recipient and the person who sent the stored communication.<sup>18</sup>

[D.11] 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'.<sup>19</sup> 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.<sup>20</sup>

### **Privacy and telecommunications**

[D.12] The *Telecommunications Act 1997* (Cth) contains a specific regime for the protection of communications.<sup>21</sup>

[D.13] Generally, carriers, carriage service providers,<sup>22</sup> 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:<sup>23</sup>

- the contents or substance of communications<sup>24</sup> that have been or are being carried<sup>25</sup> by carriers or carriage service providers;
- carriage services supplied or intended to be supplied by carriers or carriage service providers; and
- the affairs<sup>26</sup> or personal particulars (including any unlisted telephone number or any address) of other persons.

18 *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).

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

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

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

22 For definitions of 'carrier', 'carriage service provider' and related terms, see n 15 above. This would include a provider of telephone or internet services.

23 *Telecommunications Act 1997* (Cth) ss 270, 276, 277, 278. The offence has a maximum penalty of two years imprisonment.

24 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.

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

26 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.

[D.14] 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.<sup>27</sup>

## Privacy

### *Right to privacy*

[D.15] In Queensland, the main objects of the *Human Rights Act 2019* include ‘to protect and promote human rights’ and ‘to help build a culture in the Queensland public sector that respects and promotes human rights’.<sup>28</sup> The Act requires public entities to act and make decisions in a way that is compatible with human rights.<sup>29</sup>

[D.16] The Act includes a right to ‘privacy and reputation’, under which individuals have a right not to have their privacy, family, home or correspondence unlawfully or arbitrarily interfered with, and not to have their reputation unlawfully attacked.<sup>30</sup> This right may be subject only to reasonable and justifiable limits.<sup>31</sup>

[D.17] The Act includes a system for dealing with human rights complaints. The Queensland Human Rights Commission is provided with wide powers to deal with complaints, including powers to compel parties to attend conciliation and to publish information about the outcomes of complaints.<sup>32</sup>

### *Information privacy*

[D.18] 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.<sup>33</sup>

<sup>27</sup> *Telecommunications Act 1997* (Cth) pt 13 divs 2–3B. See also Lloyd, Von Thien and Ward, above n 2, [610,700].

<sup>28</sup> *Human Rights Act 2019* (Qld) s 3(a)–(b). The third object is ‘to help promote a dialogue about the nature, meaning and scope of human rights’: s 3(c).

<sup>29</sup> *Human Rights Act 2019* (Qld) s 4(b), pt 3 div 4. The term ‘public entity’ includes, for example, a government entity within the meaning of s 24 of the *Public Service Act 2008* (Qld), the Queensland Police Service and a local government: s 9.

<sup>30</sup> *Human Rights Act 2019* (Qld) ss 11, 25. This right is based on art 17 of the ICCPR: see QLRC Consultation Paper No 77 (2018) app E [E.1]–[E.5].

<sup>31</sup> *Human Rights Act 2019* (Qld) s 13. The Act provides a non-exhaustive list of factors that may be relevant in determining whether a limit is reasonable and justifiable: s 13(2).

<sup>32</sup> *Human Rights Act 2019* (Qld) pt 4.

<sup>33</sup> See, eg, *Information Privacy Act 2014* (ACT); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Act 2002* (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, the Privacy Committee of South Australia has been established to handle complaints related to the compliance of State Government agencies with a set of Information Privacy Principles. In Western Australia, some privacy principles are included in the *Freedom of Information Act 1992* (WA). See generally OAIC, Australian Government, *Privacy in your state* <<https://www.oaic.gov.au/privacy/privacy-in-your-state/>>.

## Queensland

[D.19] In Queensland, the IP Act regulates the way in which Queensland government agencies (for example, Ministers, departments, local governments and public authorities)<sup>34</sup> collect, store, use or disclose personal information.

[D.20] 'Personal information' is defined in the IP Act as:<sup>35</sup>

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.

[D.21] The IP Act imposes a general obligation on Queensland government agencies to comply with the Information Privacy Principles ('IPPs').<sup>36</sup> 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);

<sup>34</sup> 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 or quasi-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').

<sup>35</sup> *Information Privacy Act 2009* (Qld) s 12. In relation to the similar definition in the *Privacy Act 1988* (Cth) s 6, see Explanatory Note, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 61, in which it was stated that:

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.

<sup>36</sup> *Information Privacy Act 2009* (Qld) s 27. The IPPs are set out in sch 3 of the Act. All agencies, except health agencies, must comply with the IPPs. Health agencies must comply with the National Privacy Principles ('NPPs'), which are set out in sch 4 of the Act: ss 26, 30–31.



- 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).

[D.22] There are a number of exceptions to IPPs 10 and 11, including if:<sup>37</sup>

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

[D.23] 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).<sup>38</sup>

[D.24] 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').<sup>39</sup>

[D.25] 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.<sup>40</sup> The Information Commissioner may issue guidelines to Queensland government agencies, including about how the IP Act should be applied and about privacy best practice.<sup>41</sup>

<sup>37</sup> *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).

<sup>38</sup> 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.

<sup>39</sup> See *Information Privacy Act 2009* (Qld) ch 5.

<sup>40</sup> See *Information Privacy Act 2009* (Qld) ch 4; OIC, *Key functions* <<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.

<sup>41</sup> *Information Privacy Act 2009* (Qld) s 135(1)(c).

[D.26] The Information Commissioner has issued guidelines about the use of camera surveillance<sup>42</sup> and the use of drones.<sup>43</sup> 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**

[D.27] Similar to Queensland legislation, the Privacy Act regulates the way in which certain entities collect or hold personal information.<sup>44</sup>

[D.28] The Privacy Act 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.<sup>45</sup> An APP entity is required to comply with the Australian Privacy Principles ('APPs') in the Act.<sup>46</sup>

[D.29] 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'.<sup>47</sup>

[D.30] The Privacy Act 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.<sup>48</sup>

[D.31] Under the notifiable data breaches scheme in the Privacy Act, 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.<sup>49</sup>

<sup>42</sup> OIC, *Guidelines—Privacy Principles: Camera Surveillance and Privacy* (1 November 2019) <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/camera-surveillance-and-privacy>>. 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 automatic number plate recognition cameras), body-worn video cameras and unmanned aerial vehicles. See also OIC, *Guidelines—Access and amendment: Managing access to digital video recordings* (5 February 2019) <<https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/processing-applications/managing-access-to-digital-video-recordings>>.

<sup>43</sup> OIC, *Guidelines—Privacy Principles: Drones and the Privacy Principles* (16 June 2018) <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/drones-and-the-privacy-principles>>. See also OIC, *Top Privacy Tips: Drones*.

<sup>44</sup> '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).

<sup>45</sup> *Privacy Act 1988* (Cth) ss 6 (definitions of 'agency', 'APP entity' and 'organisation'), 6C–6FB.

<sup>46</sup> *Privacy Act 1988* (Cth) ss 14, 15, sch 1.

<sup>47</sup> *Privacy Act 1988* (Cth) sch 1, APP 1, 3, 7.

<sup>48</sup> *Privacy Act 1988* (Cth) pt V.

<sup>49</sup> *Privacy Act 1988* (Cth) pt IIIC.

## Criminal offences

[D.32] In Queensland, some serious breaches of privacy are recognised by the criminal law.

### *Observations or recordings in breach of privacy*

[D.33] Section 227A of the Criminal Code contains two separate offences about observing or recording a person in breach of their privacy.<sup>50</sup>

[D.34] 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.<sup>51</sup> 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 place' is a place where a person might reasonably be expected to be engaging in a private act.<sup>52</sup>

[D.35] 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.<sup>53</sup>

[D.36] Where the observation or recording is of a person engaging in a private act or a 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.<sup>54</sup>

### *Distribution of images or recordings*

[D.37] Section 227B of the Criminal Code makes it an offence to distribute or threaten to distribute a 'prohibited visual recording' of a person without the person's consent. For the purposes of this offence, a prohibited visual recording is a visual recording of the kind described in [D.34] or [D.35] above.<sup>55</sup>

[D.38] 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 the person's genital or anal region (bare or

<sup>50</sup> Criminal Code (Qld) ss 227A(1), (2). These offences have a maximum penalty of three years imprisonment.

<sup>51</sup> 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.

<sup>52</sup> 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.

<sup>53</sup> Criminal Code (Qld) s 227A(2), (3).

<sup>54</sup> Criminal Code (Qld) s 227A(1)(b)(ii), (2)(b). This requirement does not apply to the observation or visual recording of a person in a private place.

<sup>55</sup> Criminal Code (Qld) ss 207A (definition of 'prohibited visual recording'), 227B(1). The offence applies if the person who distributes the recording has reason to believe that it is a prohibited visual recording. Section 227B has a maximum penalty of three years imprisonment.

covered only by underwear).<sup>56</sup> With some exceptions,<sup>57</sup> it is also 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.<sup>58</sup>

[D.39] It is also 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 applies if the threat is made in a way that would cause fear, reasonably arising in all the circumstances, of the threat being carried out.<sup>59</sup>

[D.40] 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.<sup>60</sup>

### Other offences

[D.41] There are also other offences that might apply.

[D.42] 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.<sup>61</sup> 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.<sup>62</sup> The commission of this offence could involve the use of surveillance devices.

<sup>56</sup> Criminal Code (Qld) s 207A (definition of 'intimate image'). 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.

<sup>57</sup> 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 (Qld) s 223(4).

<sup>58</sup> Criminal Code (Qld) s 223(1). The offence has a maximum penalty of three years imprisonment. '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: s 223(2), (5). It is immaterial whether the person who distributes the intimate image intends to cause, or actually causes, the other person distress. 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.

<sup>59</sup> Criminal Code (Qld) s 229A(1), (2). The offence has a maximum penalty of three years imprisonment. '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: s 229A(4)–(5). It is immaterial whether the intimate image or prohibited visual recording exists or does not exist, or whether the person who makes the threat intends to cause, or actually causes, the fear: s 229A(3). Examples of relevant circumstances include the circumstances surrounding the threat and the relationship between the persons involved.

<sup>60</sup> See, eg, *Crimes Act 1900* (ACT) s 61B, 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; Criminal Code (WA) ch XXVA.

<sup>61</sup> Criminal Code (Qld) s 359B(c)(i), (iii).

<sup>62</sup> Criminal Code (Qld) s 359B(a), (b). See also the discussion in QLRC, *Review of termination of pregnancy laws*, Report No 76 (2018) [5.11]–[5.14].

[D.43] 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.<sup>63</sup>

[D.44] 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.<sup>64</sup> The 'use' of a restricted computer includes accessing or altering information 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 damage or gaining a benefit.<sup>65</sup> It is a defence to a charge under this offence provision to prove that the use of the restricted computer was authorised, justified or excused by law.<sup>66</sup>

[D.45] The use of surveillance might also involve trespass. 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,<sup>67</sup> or to gain entry by force, threats, intimidation, deceit or fraudulent means,<sup>68</sup> unless the entry was authorised, justified or excused by law or was made to protect the house or a person inside.<sup>69</sup> General offences of trespass apply under the *Summary Offences Act 2005* and the Criminal Code.<sup>70</sup>

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

64 Criminal Code (Qld) s 408E(1). The offence has a maximum penalty of two years imprisonment. 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 XXVIII 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.

65 If the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit, the person commits a crime and is liable to imprisonment for five years: Criminal Code (Qld) s 408E(2). If the person causes a detriment or damage or obtains a benefit for any person to the value of more than \$5000, or intends to commit an indictable offence, the person commits a crime and is liable to imprisonment for 10 years: s 408E(3).

66 Criminal Code (Qld) s 408E(4).

67 *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 (\$2669) or one year imprisonment.

68 *Invasion of Privacy Act 1971* (Qld) s 48A(1A). The offence is punishable on summary conviction by a fine of up to 30 penalty units (\$4003.50) or 18 months imprisonment.

69 *Invasion of Privacy Act 1971* (Qld) s 48A(2). 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) pt III, is regulated under different legislation: see *Security Providers Act 1993* (Qld); *Fair Trading Inspectors Act 2014* (Qld); *Privacy Act 1988* (Cth) pt IIIA.

70 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. The offence has a maximum penalty of 20 penalty units (\$2669) or one year imprisonment. See also 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. The offence has a maximum penalty of 10 years imprisonment. See also Criminal Code ss 421(2), (3), 427(2) for more serious offences.

## Common law

[D.46] In limited circumstances, a number of common law actions may indirectly protect against surveillance by protecting other interests, such as those in property.

[D.47] 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.<sup>71</sup> 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.<sup>72</sup> 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 follows or watches or keeps a person under surveillance without any threat, or who remains outside the land to carry out surveillance’.<sup>73</sup>

[D.48] An owner or occupier of land<sup>74</sup> 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.<sup>75</sup> 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’.<sup>76</sup>

<sup>71</sup> See generally *Plenty v Dillon* (1991) 171 CLR 635, 639 and the cases cited there; *Coco v The Queen* (1994) 179 CLR 427, 435; Thomson Reuters, *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].

<sup>72</sup> ALRC Discussion Paper No 80 (2014) [3.38]–[3.39]; Hinchcliffe, above n 71, 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.

<sup>73</sup> 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 71, 157.

<sup>74</sup> 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 LexisNexis Australia, *Halsbury’s Laws of Australia*, ‘Private Nuisance’ (18 November 2019) [415-640].

<sup>75</sup> *Ibid* [415-620] ff.

<sup>76</sup> ALRC Discussion Paper No 80 (2014) [3.37]; Hinchcliffe, above n 71, 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 a remotely piloted aircraft might operate without intrusion or unreasonable interference: see, eg, Handel, above n 72, 64–5; Joint Working Group Report (2003) 349.

[D.49] An action for breach of confidence can protect against the misuse or disclosure of 'confidential information'<sup>77</sup> where:<sup>78</sup>

- the confidential information is specifically identified;
- the information has the necessary quality of confidence, meaning it must not, for example, be common knowledge, be in the public domain or be trivial;
- the information was received in circumstances importing an obligation of confidence;<sup>79</sup> and
- there is an actual or threatened misuse of the information.<sup>80</sup>

### Guidelines about surveillance

[D.50] 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.<sup>81</sup>

[D.51] 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.<sup>82</sup>

<sup>77</sup> '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]; *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.

<sup>78</sup> *Optus Networks Pty Ltd v Telstra Corporation Ltd* (2010) 265 ALR 281 [39]; *Ramsay Health Care Ltd v Information Commissioner* [2019] QCATA 66 [94], [95]. See also Thomson Reuters, *The Laws of Australia*, 'Breach of Confidence' (1 November 2013) [21.11.650]; Office of the Information Commissioner (Queensland), *Guidelines—Breach of confidence* (10 December 2019) <<https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/decision-making/exempt-information-provisions/breach-of-confidence>>.

<sup>79</sup> One commentator has stated, in relation to remotely piloted aircraft ('RPA'), 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 72, 65, considering *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255.

<sup>80</sup> 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 72, 65.

<sup>81</sup> Additionally, that type of use may not be regulated by the IP Act because that legislation applies only to government agencies and if the surveillance captures 'personal information': see [D.19], [D.27]–[D.28] above; VLRC Report No 18 (2010) [3.13]–[3.17]. The position may be different in New South Wales, where regulation of optical surveillance devices applies to all activities: see [5.183] above.

<sup>82</sup> 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 [D.26] above in relation to guidelines issued by the OIC. 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–AS 4806.3) (2006, reviewed 2015); (AS 4806.4) (2008).





# Appendix E

## Civil surveillance law reform reviews and other inquiries in other jurisdictions

[E.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);
- D Stewart, 'Review of ACT Civil Surveillance Regulation' (Report, June 2016).

### New South Wales Law Reform Commission

[E.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.<sup>1</sup>

[E.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.<sup>2</sup>

[E.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

---

<sup>1</sup> 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].

<sup>2</sup> NSWLRC Interim Report No 98 (2001) [2.15]–[2.19], [2.33]–[2.39], Recs 1 to 3. See further [4.21]–[4.22] above; QLRC Consultation Paper No 77 (2018) [3.35]–[3.37].

and did not encompass all potentially invasive surveillance activity, and therefore that they did not sufficiently protect privacy.<sup>3</sup>

[E.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).<sup>4</sup>

[E.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.<sup>5</sup>

[E.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.<sup>6</sup> 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').<sup>7</sup>

[E.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.<sup>8</sup>

[E.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.<sup>9</sup>

[E.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

---

<sup>3</sup> Ibid [2.20]–[2.27].

<sup>4</sup> Ibid [2.77]–[2.79], [2.88], Recs 9, 10, 13.

<sup>5</sup> Ibid [2.86]–[2.87] and see generally chs 3, 4.

<sup>6</sup> Ibid [2.32], [2.89]–[2.98] and see respectively chs 5, 6, 7.

<sup>7</sup> Ibid [2.99]–[2.107], Rec 14 and see app A. See further QLRC Consultation Paper No 77 (2018) [3.85] ff.

<sup>8</sup> Ibid [2.28]–[2.32].

<sup>9</sup> Ibid [2.68]–[2.73], Recs 6, 7.

legislation generally maintained the traditional regulatory approach, but modernised and clarified the law.<sup>10</sup>

### Victorian Law Reform Commission

[E.11] In 2010, the VLRC completed a review on surveillance in public places.<sup>11</sup> This was the second part of a two stage reference about privacy.<sup>12</sup>

[E.12] This review was limited to a consideration of whether there is appropriate control of surveillance in public places.<sup>13</sup> 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’.<sup>14</sup>

[E.13] The VLRC therefore recommended principles-based regulation to promote the responsible use of surveillance in public places.<sup>15</sup> In particular, it recommended that legislation should include the following six overarching principles to guide all users about responsible use of public place surveillance:<sup>16</sup>

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.

<sup>10</sup> See the *Surveillance Devices Act 2007* (NSW), which replaced the *Listening Devices Act 1984* (NSW).

<sup>11</sup> 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).

<sup>12</sup> 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>>.

<sup>13</sup> 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].

<sup>14</sup> VLRC Report No 18 (2010) [4.138]–[4.141].

<sup>15</sup> 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’: at 12.

<sup>16</sup> Ibid [5.1], [5.4] ff, Rec 2.

6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

[E.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 surveillance, including by developing best practice guidelines and providing advice to ensure compliance.<sup>17</sup>

[E.15] At the same time, the VLRC recognised that ‘guidance alone cannot protect people from some practices that seriously affect their privacy’.<sup>18</sup> 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;<sup>19</sup>
- 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;<sup>20</sup>
- 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;<sup>21</sup>
- 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;<sup>22</sup>

<sup>17</sup> Ibid 13, Recs 3 to 9. The VLRC recommended that the functions of the regulator should be exercised by the Victorian Privacy Commissioner.

<sup>18</sup> Ibid [5.3], 13.

<sup>19</sup> 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.

<sup>20</sup> Ibid [6.24]–[6.28], Rec 13. The VLRC noted that this is in keeping with public expectations.

<sup>21</sup> 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): at [6.56]–[6.57].

<sup>22</sup> 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.

- 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;<sup>23</sup> and
- 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.<sup>24</sup>

[E.16] The VLRC recommended that a civil penalty regime should also apply to the criminal offences in the Act.<sup>25</sup> The regulator would be able to seek civil penalties for contraventions of the principal offences in the Act, when this course is preferable to criminal prosecutions.<sup>26</sup>

[E.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.<sup>27</sup>

### Australian Law Reform Commission

[E.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’.<sup>28</sup>

[E.19] The ALRC report, released in 2014, considered a range of matters relating to the protection of privacy,<sup>29</sup> including surveillance devices legislation.<sup>30</sup>

<sup>23</sup> 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.

<sup>24</sup> Ibid [6.94] ff, Recs 20, 21. See further [7.27]–[7.30] above; QLRC Consultation Paper No 77 (2018) [3.253] ff.

<sup>25</sup> Ibid [6.82] ff, Recs 19, 21.

<sup>26</sup> Ibid [5.44]. See further QLRC Consultation Paper No 77 (2018) [3.229], [3.316]–[3.317].

<sup>27</sup> 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>>.

<sup>28</sup> 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.

<sup>29</sup> 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*.

<sup>30</sup> See ALRC Report No 123 (2014) ch 14.

[E.20] Relevantly, the ALRC made seven recommendations about surveillance devices legislation, namely, for:<sup>31</sup>

- 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 devices (such as drones) and technologies which are not ‘devices’ in the traditional sense (such as software or networked systems);<sup>32</sup>
- 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;<sup>33</sup> and
- conferral of jurisdiction on state and territory courts or tribunals to hear disputes between residential neighbours about the use of surveillance devices.<sup>34</sup>

[E.21] The ALRC concluded that ‘the existing, technology specific laws lead to inadequate protections from surveillance’.<sup>35</sup> Overall, the ALRC observed that:<sup>36</sup>

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.

[E.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

<sup>31</sup> Ibid Recs 14-1 to 14-8. Rec 14-6 related to workplace surveillance laws and is not considered here.

<sup>32</sup> See further [4.23]–[4.24] above; QLRC Consultation Paper No 77 (2018) [3.39]–[3.42].

<sup>33</sup> ALRC Report No 123 (2014) Recs 14-1, 14-7, [14.86] ff. See further [8.14], [8.24] ff above; QLRC Consultation Paper No 77 (2018) [3.278]–[3.280].

<sup>34</sup> ALRC Report No 123 (2014) Rec 14-8, [14.90]. See further QLRC Consultation Paper No 77 (2018) [3.305]–[3.306].

<sup>35</sup> ALRC Report No 123 (2014) [14.33].

<sup>36</sup> Ibid [14.9] and see [14.1]–[14.2].

surveillance as well as surveillance by law enforcement agencies, with the latter reflecting national model provisions to facilitate cross-border investigations.<sup>37</sup>

### Australian Capital Territory review

[E.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’).<sup>38</sup>

[E.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:<sup>39</sup>

- 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 unmanned aerial vehicle (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;

<sup>37</sup> In Queensland, the law enforcement provisions are included in separate legislation: see [2.40]–[2.43] above.

<sup>38</sup> 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) <<https://www.justice.act.gov.au/review-civil-surveillance-act>>.

<sup>39</sup> ACT Review (2016) [2.5](a)–(i), [6.9]–[6.11] and see pt 6.

- 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
- preserve the court's discretion to admit evidence obtained through the use of a surveillance device in certain circumstances.

[E.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.<sup>40</sup>

[E.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.<sup>41</sup> The recommendations have not been implemented.

---

<sup>40</sup> Ibid [2.5](j), [6.46]–[6.47].

<sup>41</sup> Justice and Community Safety Directorate (ACT), *Review of Civil Surveillance in the ACT* (2016) <<https://www.justice.act.gov.au/review-civil-surveillance->



## **Appendix F**

### **Draft Surveillance Devices Bill 2020**

The draft Surveillance Devices Bill 2020 gives effect to the recommendations made in this Report.





Queensland

# Surveillance Devices Bill 2020

## Contents

		Page
<b>Part 1</b>	<b>Preliminary</b>	
<b>Division 1</b>	<b>Introduction</b>	
1	Short title . . . . .	8
2	Purpose of Act . . . . .	8
3	Act binds all persons . . . . .	9
4	Relationship with other laws . . . . .	9
<b>Division 2</b>	<b>Interpretation</b>	
5	Definitions . . . . .	9
6	Meaning of surveillance device . . . . .	9
7	Meaning of listening device . . . . .	10
8	Meaning of optical surveillance device . . . . .	10
9	Meaning of tracking device . . . . .	10
10	Meaning of data surveillance device . . . . .	10
11	Meaning of private conversation . . . . .	11
12	Meaning of private activity . . . . .	11
13	Meaning of party to a private conversation or private activity . . . . .	12
14	Meaning of surveillance information . . . . .	12
15	References to installing surveillance device . . . . .	12
16	References to owner of vehicle, computer or other thing . . . . .	12
17	References to surveillance device complaint . . . . .	13
<b>Part 2</b>	<b>Prohibitions</b>	
<b>Division 1</b>	<b>Using, installing and maintaining surveillance devices</b>	
18	Prohibition relating to listening device . . . . .	13
19	Prohibition relating to optical surveillance device . . . . .	13
20	Prohibition relating to tracking device . . . . .	14
21	Prohibition relating to data surveillance device . . . . .	14

DRAFT

## Surveillance Devices Bill 2020

## Contents

<b>Division 2</b>	<b>Exceptions relating to use, installation and maintenance of surveillance devices</b>	
22	Protection of lawful interests . . . . .	15
23	Reasonably necessary in the public interest . . . . .	15
24	Evidence of serious threat to individuals or property . . . . .	16
25	Locate lost or stolen vehicle or other thing . . . . .	16
26	Otherwise authorised . . . . .	17
<b>Division 3</b>	<b>Possessing surveillance information</b>	
27	Possessing surveillance information obtained in contravention of Act prohibited . . . . .	17
<b>Division 4</b>	<b>Communicating or publishing surveillance information</b>	
28	Surveillance information about private conversation or private activity . . . . .	18
29	Surveillance information about geographical location of individual, vehicle or other thing . . . . .	19
30	Surveillance information about information input into, output from or stored in computer . . . . .	19
31	Exceptions to offence against ss 28, 29 and 30 . . . . .	20
<b>Division 5</b>	<b>General</b>	
32	Non-publication orders . . . . .	21
33	Court may order forfeiture or destruction . . . . .	21
<b>Part 3</b>	<b>General obligations not to interfere with surveillance privacy of individuals</b>	
34	Definitions for part . . . . .	23
35	Matters relevant to whether individual has reasonable expectation of surveillance privacy . . . . .	23
36	General obligation—use of surveillance device not to interfere with individual's surveillance privacy . . . . .	25
37	General obligation—communication or publication of surveillance information not to interfere with individual's surveillance privacy . . . . .	25
38	Exceptions to contravention of general obligation . . . . .	26
<b>Part 4</b>	<b>Surveillance device complaints</b>	
<b>Division 1</b>	<b>Making and referring surveillance device complaints to commissioner</b>	
39	Meaning of surveillance device complaint . . . . .	26
40	Who may make a surveillance device complaint . . . . .	26
41	Referral entity may refer complaint . . . . .	27
42	Form of surveillance device complaint . . . . .	27
43	Time for making surveillance device complaint . . . . .	28

<b>Division 2</b>	<b>Dealing with surveillance device complaints</b>	
<b>Subdivision 1</b>	<b>General</b>	
44	Dealing with complaints . . . . .	28
45	Preliminary inquiries . . . . .	29
46	Notice of complaint . . . . .	29
47	Direction to protect privacy of complainant or respondent . . . . .	30
<b>Subdivision 2</b>	<b>Refusing to deal with surveillance device complaints</b>	
48	Refusing to deal with complaint . . . . .	30
49	Notice about refusing to deal with complaint . . . . .	31
50	When complaint lapses . . . . .	31
<b>Subdivision 3</b>	<b>Referring surveillance device complaints to other entities</b>	
51	Commissioner may refer complaint to other entities . . . . .	32
52	Commissioner may enter into arrangements with other entities . . . . .	33
<b>Division 3</b>	<b>Mediation of surveillance device complaints</b>	
53	Purpose of mediation . . . . .	33
54	Mediation of complaint . . . . .	34
55	Notice about mediation of complaint . . . . .	35
56	Confidentiality of mediation . . . . .	35
57	Evidence from mediation . . . . .	36
58	Mediated agreement . . . . .	36
59	Mediated agreement filed with QCAT . . . . .	37
<b>Division 4</b>	<b>Referral of complaints to QCAT</b>	
60	Application of division . . . . .	37
61	Notice about referring complaint to QCAT . . . . .	38
62	Referral to QCAT . . . . .	38
63	Parties to QCAT proceeding . . . . .	38
64	Constitution of QCAT for proceeding . . . . .	38
65	Deciding complaint . . . . .	39
<b>Part 5</b>	<b>Surveillance Devices Commissioner and Surveillance Devices Commission</b>	
<b>Division 1</b>	<b>Establishment</b>	
66	Surveillance Devices Commissioner and Surveillance Devices Commission . . . . .	40
67	Commission is a statutory body . . . . .	40

DRAFT

## Surveillance Devices Bill 2020

## Contents

<b>Division 2</b>	<b>Surveillance Devices Commissioner</b>	
<b>Subdivision 1</b>	<b>General</b>	
68	Functions and powers generally . . . . .	41
69	How commissioner must act . . . . .	41
70	Commissioner not subject to direction . . . . .	41
71	Control of commission . . . . .	41
<b>Subdivision 2</b>	<b>Functions and power</b>	
72	Complaints function . . . . .	42
73	Guidance functions . . . . .	42
74	Research, advice and monitoring functions . . . . .	43
75	Compliance monitoring functions . . . . .	43
76	Power to ask or direct person to give information . . . . .	45
<b>Subdivision 3</b>	<b>Appointment and related matters</b>	
77	Appointment . . . . .	45
78	Term and conditions of appointment . . . . .	46
79	Vacancy in office . . . . .	46
80	Removal from office . . . . .	46
81	Preservation of rights of public service employee appointed as commissioner . . . . .	47
82	Preservation of rights of commissioner appointed as public service employee . . . . .	48
<b>Division 3</b>	<b>Staff of the commission</b>	
83	Staff . . . . .	48
<b>Division 4</b>	<b>Reporting requirements</b>	
84	Annual report . . . . .	48
85	Other reports . . . . .	49
86	Report containing personal information . . . . .	50
87	Report containing adverse comment . . . . .	50
<b>Part 6</b>	<b>Protections</b>	
88	Protection of commissioner from civil liability . . . . .	51
89	Protection of other persons from civil, criminal and administrative liability . . . . .	51
90	No communication of official information to court . . . . .	51
<b>Part 7</b>	<b>Offences</b>	
91	Confidentiality . . . . .	52
92	False or misleading information . . . . .	53

Contents

<b>Part 8</b>	<b>General</b>	
93	Delegations . . . . .	54
94	Regulation-making power . . . . .	54
95	Review of Act . . . . .	55
<b>Part 9</b>	<b>Repeal</b>	
96	Repeal . . . . .	55
<b>Part 10</b>	<b>Transitional provision for repeal of Invasion of Privacy Act 1971</b>	
97	Proceedings for offences . . . . .	55
<b>Schedule 1</b>	<b>Dictionary . . . . .</b>	<b>57</b>

DRAFT





**2020**

---

## **A Bill**

for

**An Act to provide for an individual's privacy to be protected from unjustified interference from the use of surveillance devices and the communication or publication of information obtained using surveillance devices, and to repeal the *Invasion of Privacy Act 1971***

---

**DRAFT**

**The Parliament of Queensland enacts—**

## **Part 1 Preliminary**

### **Division 1 Introduction**

#### **1 Short title**

This Act may be cited as the *Surveillance Devices Act 2020*.

#### **2 Purpose of Act**

- (1) The purpose of this Act is to protect the privacy of individuals from unjustified interference from—
  - (a) the use of surveillance devices; and
  - (b) the communication or publication of information obtained using surveillance devices.
- (2) The purpose is to be achieved by—
  - (a) regulating the use of surveillance devices and the communication and publication of information obtained using surveillance devices; and
  - (b) imposing general obligations on persons who use surveillance devices and communicate or publish information obtained using surveillance devices; and
  - (c) providing for complaints about contraventions of these general obligations to be made and resolved; and
  - (d) providing for the Surveillance Devices Commissioner to carry out particular functions under this Act, including, for example—
    - (i) promoting understanding of and compliance with this Act, including the general obligations; and

- (ii) monitoring developments in surveillance device technology and the use of surveillance devices in civil society.

### **3 Act binds all persons**

- (1) This Act binds all persons, including the State.  
(2) However, the State can not be prosecuted for an offence against this Act.

### **4 Relationship with other laws**

This Act does not affect—

- (a) the operation of the *Information Privacy Act 2009*; or  
(b) the operation of another law regulating the use of surveillance devices; or

*Examples of other laws regulating the use of surveillance devices—*

- the *Crime and Corruption Act 2001*, chapter 3, part 6
  - the *Police Powers and Responsibilities Act 2000*, chapter 13
- (c) the power of a court to make a decision about the admissibility of information obtained using a surveillance device as evidence in a proceeding.

DRAFT

## **Division 2 Interpretation**

### **5 Definitions**

The dictionary in schedule 1 defines particular words used in this Act.

### **6 Meaning of *surveillance device***

Each of the following devices is a *surveillance device*—

- (a) a listening device;

[s 7]

---

- (b) an optical surveillance device;
- (c) a tracking device;
- (d) a data surveillance device;
- (e) a device that is a combination of 2 or more of the devices mentioned in paragraphs (a) to (d).

**7 Meaning of *listening device***

- (1) A *listening device* is a device capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation.
- (2) However, a *listening device* does not include a hearing aid or similar device used by an individual with impaired hearing.

**8 Meaning of *optical surveillance device***

- (1) An *optical surveillance device* is a device capable of being used to observe, monitor or visually record an activity.
- (2) However, an *optical surveillance device* does not include spectacles, contact lenses or a similar device used by an individual with impaired vision.

**9 Meaning of *tracking device***

A *tracking device* is a device capable of being used to find, monitor or record the geographical location of an individual, vehicle or other thing.

**10 Meaning of *data surveillance device***

A *data surveillance device* is a device or program capable of being used to access, monitor or record information that is input into, output from, or stored in a computer.

## 11 Meaning of *private conversation*

- (1) Words spoken by an individual are a *private conversation* if the words are spoken in circumstances that may reasonably be taken to indicate that—
  - (a) for words not spoken to anyone else—the individual does not want anyone else to listen to the words; or
  - (b) for words spoken to another individual, or other individuals—the individual, or at least 1 of the individuals to whom the words are spoken, does not want the words to be listened to by anyone other than—
    - (i) the individual speaking the words; and
    - (ii) the individuals to whom the words are spoken; and
    - (iii) any other individual who has the consent of all of the individuals mentioned in subparagraphs (i) and (ii).
- (2) However, a *private conversation* does not include words spoken by an individual in circumstances in which the individual, and all of the individuals to whom the words are spoken, ought reasonably to expect that someone else may listen to, monitor or record the words.

## 12 Meaning of *private activity*

- (1) An activity is a *private activity* if it is carried out in circumstances that may reasonably be taken to indicate that—
  - (a) for an activity carried out by 1 individual—the individual does not want anyone else to observe the activity; or
  - (b) for an activity carried out by 2 or more individuals—at least 1 of the individuals does not want the activity to be observed by anyone other than—
    - (i) the individuals carrying out the activity; and
    - (ii) any other individual who has the consent of all of the individuals carrying out the activity.

[s 13]

---

- (2) However, a *private activity* does not include an activity carried out by 1 or more individuals in circumstances in which all of the individuals carrying out the activity ought reasonably to expect that someone else may observe, monitor or visually record the activity.

**13 Meaning of *party* to a private conversation or private activity**

- (1) Each of the following is a *party* to a private conversation—
- (a) an individual who speaks, or is spoken to, during the conversation;
  - (b) an individual who listens to the conversation with the consent of all of the individuals mentioned in paragraph (a).
- (2) Each of the following is a *party* to a private activity—
- (a) an individual carrying out the activity;
  - (b) an individual who observes the activity with the consent of all of the individuals mentioned in paragraph (a).

**14 Meaning of *surveillance information***

*Surveillance information* is information obtained, directly or indirectly, using a surveillance device.

**15 References to installing surveillance device**

In this Act, a reference to installing a surveillance device includes doing anything to, or in relation to, a device to enable it to be used as a surveillance device.

**16 References to owner of vehicle, computer or other thing**

In this Act, a reference to a person who owns a vehicle, computer or other thing does not include a person (an

*excluded owner*) who owns the vehicle, computer or other thing if—

- (a) another person has the use or control of the vehicle, computer or other thing under a credit agreement, hiring agreement, hire-purchase agreement, leasing agreement or another similar agreement; and
- (b) under the agreement, the excluded owner is not entitled to immediate possession of the vehicle, computer or other thing.

## **17 References to surveillance device complaint**

In this Act, a reference to a surveillance device complaint includes a reference to a part of a surveillance device complaint.

# **Part 2 Prohibitions**

## **Division 1 Using, installing and maintaining surveillance devices**

### **18 Prohibition relating to listening device**

A person must not use, install or maintain a listening device to listen to, monitor or record a private conversation without the consent of each party to the conversation.

Maximum penalty—60 penalty units or 3 years imprisonment.

### **19 Prohibition relating to optical surveillance device**

A person must not use, install or maintain an optical surveillance device to observe, monitor or visually record a

DRAFT

[s 20]

---

private activity without the consent of each party to the activity.

Maximum penalty—60 penalty units or 3 years imprisonment.

## **20 Prohibition relating to tracking device**

- (1) A person must not use, install or maintain a tracking device to find, monitor or record the geographical location of an individual without the consent of the individual.

Maximum penalty—60 penalty units or 3 years imprisonment.

- (2) A person must not use, install or maintain a tracking device to find, monitor or record the geographical location of a vehicle or other thing without the consent of each person who owns, or is in lawful control of, the vehicle or thing.

Maximum penalty—60 penalty units or 3 years imprisonment.

## **21 Prohibition relating to data surveillance device**

A person must not use, install or maintain a data surveillance device to access, monitor or record information that is input into, output from or stored in a computer without the consent of each person who owns, or is in lawful control of, the computer.

Maximum penalty—60 penalty units or 3 years imprisonment.

DRAFT



---

**Division 2**                      **Exceptions relating to use,  
installation and maintenance of  
surveillance devices**

**22**            **Protection of lawful interests**

A person who uses, installs or maintains a surveillance device does not commit an offence against section 18, 19, 20 or 21 if use of the device is reasonably necessary to protect the lawful interests of—

- (a) the person; or
- (b) if another person has authorised the person to use the surveillance device on the other person's behalf—the other person.

**23**            **Reasonably necessary in the public interest**

- (1) A person who uses, installs or maintains a surveillance device does not commit an offence against section 18, 19, 20 or 21 if use of the device is reasonably necessary in the public interest.
- (2) In deciding whether the use of a surveillance device is reasonably necessary in the public interest, a court must consider the following matters as they existed when the person used, installed or maintained the device—
  - (a) the subject matter of the use of the device;
  - (b) the information that the person reasonably expected would be obtained from the use of the device;
  - (c) the purpose for which the person intended to use information that the person reasonably expected would be obtained from the use of the device;
  - (d) the nature of the public interest that arose in the circumstances;
  - (e) whether the public interest could have been served in another reasonable way;

DRAFT

[s 24]

---

- (f) the extent to which the use, installation or maintenance of the device affected, or was likely to affect, the privacy of an individual;
- (g) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

## **24 Evidence of serious threat to individuals or property**

- (1) A person who uses, installs or maintains a surveillance device to obtain evidence of, or information about, a serious threat does not commit an offence against section 18, 19, 20 or 21 if the person believes, on reasonable grounds, it is necessary for the device to be used immediately to obtain the evidence or information.
- (2) In this section—  
*serious threat* means—
  - (a) a serious threat to the life, health, safety or wellbeing of an individual; or
  - (b) a serious threat of substantial damage to property.

## **25 Locate lost or stolen vehicle or other thing**

A person who uses a surveillance device to locate a vehicle or other thing does not commit an offence against section 18, 19, 20 or 21 if the person—

- (a) is not in possession or control of the vehicle or thing; and
- (b) believes, on reasonable grounds, that the vehicle or thing is lost or stolen; and
- (c) is an owner of the vehicle or thing or, before the vehicle or thing was lost or stolen, was in lawful control of it.

**26 Otherwise authorised**

A person who uses, installs or maintains a surveillance device does not commit an offence against section 18, 19, 20 or 21 if the use, installation or maintenance is—

- (a) authorised under another Act of the State or an Act of the Commonwealth; or
- (b) in circumstances prescribed by regulation for this section.

**Division 3 Possessing surveillance information**

**27 Possessing surveillance information obtained in contravention of Act prohibited**

- (1) A person must not, without the consent of each relevant person, possess information that the person knows is surveillance information obtained in contravention of section 18, 19, 20 or 21.

Maximum penalty—20 penalty units or 1 year's imprisonment.

- (2) However, a person does not commit an offence against subsection (1) if the person—
- (a) possesses the information in relation to proceedings for an offence against this Act; or
  - (b) possesses the information because it was communicated to the person, or published, in a way that does not contravene this Act.

- (3) In this section—

***relevant person***, in relation to surveillance information, means—

DRAFT

[s 28]

---

- (a) if the surveillance information is about a private conversation obtained using a listening device—each party to the conversation; or
- (b) if the surveillance information is about a private activity obtained using an optical surveillance device—each party to the activity; or
- (c) if the surveillance information is about the geographical location of an individual obtained using a tracking device—the individual; or
- (d) if the surveillance information is about the geographical location of a vehicle or other thing obtained using a tracking device—each person who owns, or is in lawful control of, the vehicle or thing; or
- (e) if the surveillance information is about the information input into, output from or stored in a computer obtained using a data surveillance device—each person who owns, or is in lawful control of, the computer.

## **Division 4                      Communicating or publishing surveillance information**

### **28            Surveillance information about private conversation or private activity**

A person must not communicate or publish surveillance information about a private conversation or private activity if the person—

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) does not have the consent of each party to the conversation or activity to communicate or publish the information.

Maximum penalty—60 penalty units or 3 years imprisonment.

**29 Surveillance information about geographical location of individual, vehicle or other thing**

A person must not communicate or publish surveillance information about the geographical location of an individual, a vehicle or another thing if the person—

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) does not have the consent of the following person or persons to communicate or publish the information—
  - (i) for information about the location of an individual—that individual;
  - (ii) for information about the location of a vehicle or other thing—each person who owns, or is in lawful control of, the vehicle or thing.

Maximum penalty—60 penalty units or 3 years imprisonment.

**30 Surveillance information about information input into, output from or stored in computer**

A person must not communicate or publish surveillance information about information that is input into, output from or stored in a computer if the person—

- (a) knows, or ought reasonably to know, the information is surveillance information; and
- (b) does not have the consent of each person who owns, or is in lawful control of, the computer to communicate or publish the information.

Maximum penalty—60 penalty units or 3 years imprisonment.

DRAFT

[s 31]

---

**31 Exceptions to offence against ss 28, 29 and 30**

- (1) A person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is—
  - (a) in a legal proceeding; or
  - (b) reasonably necessary to protect the lawful interests of—
    - (i) the person; or
    - (ii) another person who has authorised the person to communicate or publish the information on the other person's behalf; or
  - (c) reasonably necessary in the public interest; or
  - (d) reasonably necessary to lessen or prevent a serious threat—
    - (i) to the life, health, safety or wellbeing of an individual; or
    - (ii) of substantial damage to property; or
  - (e) authorised under another Act of the State or an Act of the Commonwealth; or
  - (f) in circumstances prescribed by regulation for this subsection.
- (2) Also, a person does not commit an offence against section 28, 29 or 30 if the use of a surveillance device to obtain the surveillance information the subject of the communication or publication was authorised under another Act of the State or an Act of the Commonwealth.
- (3) For deciding whether a person's communication or publication of surveillance information is reasonably necessary in the public interest for subsection (1)(c), a court must consider the following matters as they existed when the person communicated or published the information—
  - (a) the subject matter of the surveillance information;
  - (b) the scope of the communication or publication;

- (c) the nature of the public interest that arose in the circumstances;
- (d) whether the public interest could have been served in another reasonable way;
- (e) the extent to which the communication or publication affected, or was likely to affect, the privacy of an individual;
- (f) whether, on balance in the circumstances, the public interest justified the interference with the privacy of an individual.

## Division 5                      General

### 32            **Non-publication orders**

- (1) This section applies to a proceeding for an offence against this part.
- (2) The court may make an order (a *non-publication order*) prohibiting the publication of evidence given before the court, other than in the way and to the persons stated in the order.
- (3) The court may make a non-publication order only if the court considers the order is necessary in the interests of justice.
- (4) The court may make a non-publication order at any time during the proceeding.
- (5) A person must not contravene a non-publication order, unless the person has a reasonable excuse.

Maximum penalty for subsection (5)—60 penalty units or 3 years imprisonment.

### 33            **Court may order forfeiture or destruction**

- (1) If a person is convicted of an offence against this Act, the court before which the person is convicted may make an order that—

DRAFT

[s 33]

---

- (a) a surveillance device used in connection with the commission of the offence is forfeited to the State; or
  - (b) a document, device or other thing that contains related information, or on which related information is stored, is forfeited to the State; or
  - (c) related information be destroyed.
- (2) Before making an order under subsection (1), the court may require notice to be given to, and hear from, a person the court considers appropriate.
- (3) Subsection (1) applies whether or not the surveillance device, document, device or thing to be forfeited, or related information to be destroyed, has been seized.
- (4) The court may also make any order that it considers appropriate to enforce the forfeiture.
- (5) This section does not limit the court's powers under the *Penalties and Sentences Act 1992*, the *Criminal Proceeds Confiscation Act 2002* or another law.
- (6) When forfeited to the State, the surveillance device, document, device or thing becomes the State's property and may be dealt with as directed by the chief executive.
- (7) In this section—  
***related information***, for an offence, means—
  - (a) information to which the offence relates; or
  - (b) information obtained using a surveillance device to which the offence relates.



## Part 3                      General obligations not to interfere with surveillance privacy of individuals

### 34        Definitions for part

In this part—

***reasonable expectation***, of surveillance privacy for an individual, means the individual is reasonably entitled to expect surveillance privacy—

- (a) in relation to a particular use of a surveillance device; or
- (b) in relation to surveillance information obtained when the individual was the subject of surveillance.

***surveillance privacy***, of an individual, means—

- (a) in relation to a particular use of a surveillance device—the individual is not the subject of surveillance from that use of a surveillance device; or
- (b) in relation to surveillance information obtained when the individual was the subject of surveillance—the surveillance information is not communicated or published.

### 35        Matters relevant to whether individual has reasonable expectation of surveillance privacy

- (1) The following matters are relevant for deciding whether an individual has a reasonable expectation of surveillance privacy in relation to the use of a surveillance device, or the communication or publication of surveillance information—
  - (a) the individual's location when the surveillance device is used;
  - (b) the subject matter of the use, or the surveillance information, including whether it is of an intimate, familial, health-related or financial nature;

DRAFT

[s 35]

---

- (c) the type of device used;
  - (d) the nature and purpose of the use, communication or publication, including, for example—
    - (i) the extent to which the use, communication or publication targets the individual; and
    - (ii) whether the use is covert; and
    - (iii) in relation to the communication or publication, how the information is communicated or published; and
    - (iv) whether the use, communication or publication contravenes a provision of an Act;
  - (e) the nature and extent of any notice given about the use;
  - (f) whether the individual has an opportunity to avoid the surveillance;
  - (g) the individual's attributes and conduct, including, for example—
    - (i) the extent to which the individual has a public profile, invites or encourages publicity or shows a wish for privacy; and
    - (ii) the extent to which the individual is in a position of vulnerability; and
    - (iii) the nature of any relationship between the individual and the person using the surveillance device, or making the communication or publication; and
    - (iv) the effect that the use, communication or publication is reasonably likely to have on the individual's health, safety or wellbeing.
- (2) Subsection (1) does not limit the matters that may be considered relevant for deciding whether an individual has a reasonable expectation of surveillance privacy in relation to the use of a surveillance device, or the communication or publication of surveillance information.

**36 General obligation—use of surveillance device not to interfere with individual’s surveillance privacy**

- (1) This section applies if an individual has a reasonable expectation of surveillance privacy in relation to a particular use of a surveillance device.
- (2) A person must not use a surveillance device in a way that interferes with the individual’s surveillance privacy.
- (3) However, a person does not contravene subsection (2) if—
  - (a) the individual has consented to the surveillance device being used in that way; or
  - (b) the person did not know, and ought not reasonably to have known, that the particular use of the device would interfere with the individual’s surveillance privacy.

**37 General obligation—communication or publication of surveillance information not to interfere with individual’s surveillance privacy**

- (1) This section applies if an individual has a reasonable expectation of surveillance privacy in relation to surveillance information.
- (2) A person must not communicate or publish the surveillance information in a way that interferes with the individual’s surveillance privacy.
- (3) However, a person does not contravene subsection (2) if—
  - (a) the individual has consented to the communication or publication; or
  - (b) the person did not know, and ought not reasonably to have known, that the communication or publication would interfere with the individual’s surveillance privacy.

DRAFT

### **38 Exceptions to contravention of general obligation**

A person does not contravene a general obligation if the person's use of a surveillance device, or communication or publication of surveillance information—

- (a) is authorised or required by law; or
- (b) is authorised or required by an order or process of a court or tribunal; or
- (c) is incidental to, and reasonably necessary for, the exercise of a lawful right to defend a person or property, including to prosecute or defend a criminal or civil proceeding; or
- (d) is reasonably necessary in the public interest and the public interest outweighs the interference with the individual's surveillance privacy.

## **Part 4 Surveillance device complaints**

### **Division 1 Making and referring surveillance device complaints to commissioner**

#### **39 Meaning of *surveillance device complaint***

A *surveillance device complaint* is a complaint about an alleged contravention of a general obligation made by or for an individual who is the subject of the alleged contravention.

#### **40 Who may make a surveillance device complaint**

- (1) An individual who is the subject of an alleged contravention of a general obligation may make a surveillance device complaint about the alleged contravention to the commissioner.

- (2) A surveillance device complaint about the alleged contravention may also be made to the commissioner for the individual by—
  - (a) an agent of the individual; or
  - (b) another person authorised by the commissioner in writing to make a complaint for the individual.
- (3) A surveillance device complaint may be made by, or for, 2 or more individuals jointly.

#### **41 Referral entity may refer complaint**

- (1) This section applies if a referral entity receives a complaint under a referral Act, or another entity receives a complaint while performing the entity's functions under a law, and considers the complaint may also be a surveillance device complaint.
- (2) The entity that receives the complaint may refer the complaint to the commissioner.

*Note—*

Under section 52, the commissioner and a referral entity may enter into an arrangement about referring complaints under a referral Act or dealing with complaints that are not referred.

#### **42 Form of surveillance device complaint**

- (1) A surveillance device complaint made or referred to the commissioner must—
  - (a) be in writing; and
  - (b) state the complainant's name and contact details, including, for example, the complainant's postal or email address; and
  - (c) if the person making or referring the complaint knows the respondent's name, address or other contact details—the respondent's name, address or other contact details; and

DRAFT

[s 43]

---

- (d) include enough information to identify the alleged contravention to which the complaint relates.
- (2) If the commissioner is satisfied the complainant needs help to put the complaint in writing, the commissioner must give the complainant reasonable help to put the complaint in writing.

#### **43 Time for making surveillance device complaint**

A surveillance device complaint must be made—

- (a) within 6 months after the alleged contravention the subject of the complaint came to the complainant's knowledge; or
- (b) within the further period that the commissioner considers is reasonable in all the circumstances.

### **Division 2 Dealing with surveillance device complaints**

#### **Subdivision 1 General**

#### **44 Dealing with complaints**

- (1) If a surveillance device complaint is made or referred to the commissioner under division 1, the commissioner must deal with the complaint under this part.
- (2) Without limiting subsection (1), the commissioner may—
  - (a) refuse to deal with, or to continue to deal with, the complaint under subdivision 2; or
  - (b) refer the complaint to a referral entity under subdivision 3; or
  - (c) try to resolve the complaint by mediation under division 3.

*Note—*

See division 4 for the circumstances in which the commissioner may refer a surveillance device complaint to QCAT to decide.

**45 Preliminary inquiries**

The commissioner may make preliminary inquiries about a surveillance device complaint made or referred to the commissioner to—

- (a) decide how to deal with the complaint under this part; or
- (b) if the complaint does not include enough information to identify the respondent to the complaint—identify the respondent.

**46 Notice of complaint**

- (1) The commissioner must give the complainant and respondent notice of a surveillance device complaint made or referred to the commissioner as soon as practicable after receiving the complaint.
- (2) The notice must state—
  - (a) the substance of the complaint; and
  - (b) the role of the commissioner in dealing with the complaint under this part; and
  - (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint; and
  - (d) for a notice to the respondent—that the respondent must advise the commissioner of the respondent’s contact details, including, for example, the respondent’s postal or email address.

DRAFT

[s 47]

---

**47 Direction to protect privacy of complainant or respondent**

- (1) This section applies if, in dealing with a surveillance device complaint under this part, the commissioner is satisfied on reasonable grounds that it is necessary to give a direction under subsection (2) to protect the privacy of the complainant or respondent.
- (2) The commissioner may, by notice given to a person, direct the person not to communicate or publish information that identifies, or is likely to identify, the complainant or respondent.
- (3) The person must comply with the direction unless the person has a reasonable excuse.

Maximum penalty—10 penalty units.

**Subdivision 2 Refusing to deal with surveillance device complaints**

**48 Refusing to deal with complaint**

- (1) The commissioner may refuse to deal with, or to continue to deal with, a surveillance device complaint if—
  - (a) the commissioner considers—
    - (i) the complaint does not comply with section 42(1)(b) or (c); or
    - (ii) there is a more appropriate course of action available under another law to deal with the subject of the complaint; or
    - (iii) the subject of the complaint has been appropriately dealt with by another entity; or
  - (b) the complaint was not made within the time required under section 43; or
  - (c) the complaint is frivolous, trivial, vexatious, misconceived or lacking in substance.



- 
- (2) The commissioner may refuse to continue to deal with a surveillance device complaint if—
- (a) the complainant does not comply with a reasonable request made by the commissioner in dealing with the complaint; or
  - (b) the commissioner is satisfied on reasonable grounds the complainant, without a reasonable excuse, has not cooperated in the commissioner's dealing with the complaint; or
  - (c) the commissioner can not make contact with the complainant.

**49 Notice about refusing to deal with complaint**

- (1) If the commissioner refuses to deal with, or to continue to deal with, a surveillance device complaint, the commissioner must give the complainant and respondent notice of the refusal and the reasons for the refusal.
- (2) However, the commissioner need not give the notice to the respondent if the commissioner considers it is not necessary to do so in the circumstances.

*Examples of circumstances—*

The respondent is not aware of the complaint or has not been contacted by the commissioner in relation to the complaint.

**50 When complaint lapses**

If the commissioner refuses to deal with, or to continue to deal with, a surveillance device complaint—

- (a) the complaint lapses; and
- (b) the complainant can not make a further complaint relating to the alleged contravention the subject of the complaint.

DRAFT

### **Subdivision 3 Referring surveillance device complaints to other entities**

#### **51 Commissioner may refer complaint to other entities**

- (1) The commissioner may refer a surveillance device complaint to a referral entity as follows—
  - (a) if the subject of the complaint could be the subject of a privacy complaint under the *Information Privacy Act 2009*—the information commissioner;
  - (b) if the subject of the complaint could be the subject of a human rights complaint under the *Human Rights Act 2019*—the human rights commissioner;
  - (c) if the subject of the complaint could be the subject of a complaint under the *Ombudsman Act 2001*—the ombudsman;
  - (d) if the subject of the complaint could be the subject of a health service complaint under the *Health Ombudsman Act 2013*—the health ombudsman.
- (2) However, the commissioner may refer a surveillance device complaint to a referral entity under this section only if—
  - (a) the complainant consents; and
  - (b) the commissioner considers the complaint would be more appropriately dealt with by the referral entity to which it is referred.
- (3) If the commissioner refers a surveillance device complaint to a referral entity under this section, the commissioner—
  - (a) may, with the consent of the complainant, give the referral entity information about the complaint obtained by the commissioner under this part; and
  - (b) must give the complainant and respondent a notice that states the complaint has been referred to the referral entity.

- (4) However, the commissioner need not give the notice to the respondent if the commissioner considers it is not necessary to do so in the circumstances.

*Examples of circumstances—*

The respondent is not aware of the complaint or has not been contacted by the commissioner in relation to the complaint.

**52 Commissioner may enter into arrangements with other entities**

- (1) The commissioner and a referral entity may enter into an arrangement about the following matters—
- (a) the types of surveillance device complaints the commissioner should refer to the entity;
  - (b) the types of complaints made under a referral Act the referral entity should refer to the commissioner;
  - (c) dealing with a complaint or other matter under a referral Act that could also form the basis of a surveillance device complaint;
  - (d) cooperating in the performance of the commissioner's and the entity's functions to ensure the effective operation of this part and a referral Act.
- (2) If an arrangement provides for a referral as mentioned in subsection (1)(a) or (b), the arrangement must also provide for how the referral is made.

DRAFT

**Division 3 Mediation of surveillance device complaints**

**53 Purpose of mediation**

The purpose of mediation of a surveillance device complaint is to—

- (a) identify and clarify the issues in the complaint; and

[s 54]

---

- (b) promote the resolution of the complaint in a way that is informal, quick and efficient.

#### **54 Mediation of complaint**

- (1) The commissioner must try to mediate a surveillance device complaint under this division if—
  - (a) in the commissioner's opinion, it is reasonably likely the complaint could be resolved by mediation; and
  - (b) the commissioner does not—
    - (i) refuse to deal with, or to continue to deal with, the complaint under division 2, subdivision 2; or
    - (ii) refer the complaint to a referral entity under division 2, subdivision 3.
- (2) The commissioner may take the reasonable action the commissioner considers appropriate to try to resolve the complaint by mediation.
- (3) Without limiting subsection (2), the commissioner may—
  - (a) ask the respondent to give the commissioner a written response to the complaint; or
  - (b) give the complainant a copy of the respondent's written response; or
  - (c) ask or direct the complainant or respondent to give the commissioner information relevant to the complaint, including under section 76; or
  - (d) make enquiries of, and discuss the complaint with, the complainant and the respondent; or
  - (e) provide information to the complainant and respondent about this Act and how it applies to the complaint; or
  - (f) facilitate a meeting between the complainant and respondent.

DRAFT

**55 Notice about mediation of complaint**

- (1) If the commissioner is required to try to mediate a surveillance device complaint under this division, the commissioner must give the complainant and respondent notice about the mediation.
- (2) The notice must state—
  - (a) the substance of the complaint; and
  - (b) the powers the commissioner may exercise in trying to resolve the complaint by mediation; and
  - (c) that the commissioner may seek information or documents from the complainant or respondent in relation to the complaint.
- (3) The notice given to the respondent must also state that the respondent will be given an opportunity to respond to the complaint in writing.

**56 Confidentiality of mediation**

- (1) This section applies in relation to a person who is, or has been, the commissioner or a staff member of the commission.
- (2) The person must not disclose information that comes to the person's knowledge during the mediation of a surveillance device complaint.
- (3) Subsection (2) does not apply if the disclosure is made—
  - (a) with the consent of the complainant and respondent to the surveillance device complaint; or
  - (b) for the purpose of giving effect to the provisions of this part or section 84 or 85; or
  - (c) for statistical purposes without identifying a person to whom the information relates; or
  - (d) for an inquiry or proceeding about an offence happening during the mediation; or

DRAFT

[s 57]

---

- (e) for a proceeding founded on fraud alleged to be connected with, or to have happened during, the mediation; or
- (f) under a requirement imposed by an Act.

## **57 Evidence from mediation**

- (1) Evidence of anything said or done, or an admission made, in the course of the mediation of a surveillance device complaint is admissible in a civil proceeding only if the complainant and respondent agree.
- (2) Subsection (1) does not apply to a mediated agreement for a surveillance device complaint prepared under section 58 if a copy of the mediated agreement is filed with QCAT under section 59.
- (3) In this section—  
*civil proceeding* does not include a civil proceeding founded on fraud alleged to be connected with, or to have happened during, the mediation.

## **58 Mediated agreement**

- (1) If, after mediation of a surveillance device complaint, the complainant and respondent agree to resolve the complaint, the agreement is not binding until it is—
  - (a) written down; and
  - (b) signed by the complainant and respondent; and
  - (c) certified by the commissioner as a mediated agreement under this section.
- (2) An agreement that complies with subsection (1) is a *mediated agreement*.
- (3) The commissioner must keep a copy of a mediated agreement for a surveillance device complaint.

**59 Mediated agreement filed with QCAT**

- (1) The complainant or respondent for a surveillance device complaint may file a copy of a mediated agreement for the complaint with QCAT.
- (2) QCAT may make an order necessary to give effect to the mediated agreement if QCAT is satisfied—
  - (a) the order is consistent with an order QCAT may make under section 65 or the QCAT Act; and
  - (b) it is practicable to implement the order.
- (3) An order under subsection (2) is, and may be enforced as, an order of QCAT under the QCAT Act.

**Division 4 Referral of complaints to QCAT**

**60 Application of division**

This division applies in relation to a surveillance device complaint made or referred to the commissioner if—

- (a) the commissioner does not—
  - (i) refuse to deal with, or to continue to deal with, the complaint under division 2, subdivision 2; or
  - (ii) refer the complaint to a referral entity under division 2, subdivision 3; and
- (b) in the commissioner's opinion, the complaint is unlikely to be resolved—
  - (i) by mediation of the complaint under division 3; or
  - (ii) despite attempts to mediate the complaint under division 3.

DRAFT

**61 Notice about referring complaint to QCAT**

The commissioner must give notice to the complainant and respondent for the complaint that states—

- (a) this division applies and why this division applies; and
- (b) that, if asked to do so by the complainant, the commissioner will refer the complaint to QCAT to decide.

**62 Referral to QCAT**

- (1) This section applies if, within 20 business days after receiving a notice from the commissioner under section 61, the complainant asks the commissioner, in writing, to refer the complaint to QCAT.
- (2) The commissioner must refer the complaint to QCAT within 20 business days after receiving the complainant's request.
- (3) QCAT is to exercise its original jurisdiction under the QCAT Act to hear and decide the complaint.

**63 Parties to QCAT proceeding**

- (1) The complainant and respondent for the complaint referred to QCAT are both parties to the proceeding before QCAT.
- (2) The complainant for the complaint is taken to be the applicant for the proceeding.
- (3) The respondent for the complaint is taken to be the respondent for the proceeding.

**64 Constitution of QCAT for proceeding**

- (1) QCAT must be constituted by at least 1 member who is a legally qualified member for a proceeding to hear and decide the complaint.
- (2) In this section—



*legally qualified member* see the QCAT Act, schedule 3.

## **65 Deciding complaint**

- (1) QCAT may make only the following final decisions to decide a surveillance device complaint—
  - (a) an order that—
    - (i) declares that the respondent's use of a surveillance device, or communication or publication of surveillance information, contravened a general obligation in relation to the complainant; and
    - (ii) if QCAT considers appropriate—includes 1 or more of the orders stated in subsection (2);
  - (b) an order dismissing the complaint;
  - (c) an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

*Note—*

See the QCAT Act, section 114 for QCAT's power to impose conditions on a decision and to make ancillary orders and directions.

- (2) For subsection (1)(a)(ii), the orders are as follows—
  - (a) an order that the respondent must not repeat or continue a stated act or practice;
  - (b) an order that the respondent must compensate the complainant for loss or damage suffered because of the respondent's act or practice, including for injury to the complainant's feelings or humiliation suffered by the complainant, by—
    - (i) engaging in a stated act or practice; or
    - (ii) paying the complainant a stated amount of not more than \$100,000.
- (3) An order under subsection (2) must state the reasonable time within which the relevant action must be taken.

DRAFT

[s 66]

---

- (4) In this section—  
*final decision*, of QCAT in a proceeding, see the QCAT Act, schedule 3.

## **Part 5                      Surveillance Devices Commissioner and Surveillance Devices Commission**

### **Division 1                      Establishment**

#### **66                      Surveillance Devices Commissioner and Surveillance Devices Commission**

- (1) There is to be a Surveillance Devices Commissioner.
- (2) The Surveillance Devices Commission is established.
- (3) The commission consists of the commissioner and the staff of the commission.

#### **67                      Commission is a statutory body**

- (1) The commission is a statutory body for the *Financial Accountability Act 2009* and the *Statutory Bodies Financial Arrangements Act 1982*.
- (2) The *Statutory Bodies Financial Arrangements Act 1982*, part 2B sets out the way in which the commissioner's powers under this Act are affected by the *Statutory Bodies Financial Arrangements Act 1982*.

## **Division 2                      Surveillance Devices Commissioner**

### **Subdivision 1              General**

#### **68              Functions and powers generally**

- (1) The commissioner has the functions and powers given by this Act.
- (2) The commissioner has power to do all things necessary or convenient to be done to perform the commissioner's functions.

#### **69              How commissioner must act**

In performing the commissioner's functions, the commissioner must act independently, impartially and in the public interest.

#### **70              Commissioner not subject to direction**

- (1) The commissioner is not subject to direction by any person about how the commissioner performs the commissioner's functions.
- (2) However, the Minister may ask the commissioner to—
  - (a) provide advice or assistance about a particular matter under section 74(d), (e) or (f); or
  - (b) prepare a report about a particular matter under section 85.

#### **71              Control of commission**

The commissioner controls the commission.

DRAFT

## **Subdivision 2      Functions and power**

### **72      Complaints function**

The commissioner's functions include receiving complaints and dealing with them under this Act.

### **73      Guidance functions**

- (1) The commissioner's functions include—
  - (a) promoting understanding of and compliance with this Act, including the general obligations; and
  - (b) providing information and guidance about the operation of this Act; and
  - (c) providing education and training about this Act, including the general obligations and the lawful use of surveillance devices; and
  - (d) issuing guidelines about any matter related to the commissioner's functions, including guidelines about—
    - (i) how this Act applies; and
    - (ii) how an exception to a prohibition under part 2 or a general obligation under part 3 applies, including examples; and
    - (iii) best practice for using surveillance devices, and communicating or publishing surveillance information, in a way that respects individuals' privacy; and
    - (iv) making, referring and dealing with complaints; and
  - (e) giving information and reasonable help to complainants and respondents to complaints in relation to their complaints and the processes under this Act.
- (2) If the commissioner issues a guideline under subsection (1)(d), the commissioner must publish the guideline on the commissioner's website.

## **74 Research, advice and monitoring functions**

The commissioner's functions include—

- (a) undertaking or commissioning research to monitor the following matters—
  - (i) whether this Act is achieving its purpose;
  - (ii) how surveillance devices and surveillance device technologies are used in civil society;
  - (iii) developments in surveillance device technology; and
- (b) identifying and commenting on issues relating to the use of surveillance devices in civil society and the communication or publication of surveillance information; and
- (c) identifying and commenting on legislative and administrative changes that would improve the operation of this Act; and
- (d) advising the Minister about matters relevant to the operation and administration of this Act, on the request of the Minister or on the commissioner's own initiative; and
- (e) on the request of the Minister, assisting the Minister to review the Act under section 95; and
- (f) on the request of the Minister, examining other Acts and proposed legislation to determine whether they are, or would be, consistent with the purpose of this Act and the general obligations.

## **75 Compliance monitoring functions**

- (1) The commissioner's functions include examining, on the commissioner's own initiative or otherwise, the practices of relevant entities in relation to the following matters to monitor whether the practices comply with this Act—
  - (a) how the entities use surveillance devices;

DRAFT

[s 75]

---

- (b) how the entities communicate or publish surveillance information;
  - (c) the surveillance device technology, and communication and publication technology, the entities use;
  - (d) the programs, policies and procedures of the entities in relation to the matters mentioned in paragraphs (a), (b) and (c).
- (2) In this section—
  - relevant entity***—
    - (a) means—
      - (i) a public entity under the *Human Rights Act 2019*; or
      - (ii) an entity with an annual turnover of more than \$5m for the current or previous financial year; or
      - (iii) an entity that regularly or routinely—
        - (A) uses a surveillance device; or
        - (B) communicates or publishes surveillance information; or
      - (iv) an entity that uses a surveillance device to monitor crowds in places that are open to, or used by the public, whether or not on the payment of a fee; or
      - (v) another entity prescribed by regulation for this definition; but
    - (b) does not include an entity to the extent the entity's practices mentioned in subsection (1) relate to enforcing a law of the State, including, for example—
      - (i) the Queensland Police Service; or
      - (ii) the Crime and Corruption Commission.

## **76 Power to ask or direct person to give information**

- (1) This section applies if the commissioner believes on reasonable grounds that a person may have information relevant to—
  - (a) a surveillance device complaint being dealt with by the commissioner under part 4; or
  - (b) another function being performed by the commissioner.
- (2) The commissioner may, by notice given to the person, ask or direct the person to give stated information to the commissioner within the reasonable period stated in the notice.
- (3) The notice must state the purpose for asking or directing the person to give the information.
- (4) For information in an electronic document, compliance with the direction requires the giving of a clear image or written version of the electronic document.
- (5) The person must comply with a direction to give information made under this section unless the person has a reasonable excuse.

Maximum penalty—10 penalty units.
- (6) It is a reasonable excuse for a person not to give the information if—
  - (a) the information is the subject of legal professional privilege; or
  - (b) if the person is an individual—giving the information might tend to incriminate the individual.

DRAFT

## **Subdivision 3 Appointment and related matters**

### **77 Appointment**

- (1) The commissioner is to be appointed by the Governor in Council.

[s 78]

---

- (2) The commissioner is appointed under this Act and not the *Public Service Act 2008*.

## **78 Term and conditions of appointment**

- (1) The commissioner holds office for the term, of not more than 5 years, and on the conditions stated in the commissioner's instrument of appointment.
- (2) However, a person being reappointed as commissioner can not be reappointed for a term that would result in the person holding office as commissioner for more than 10 years continuously.
- (3) The commissioner is to be paid the remuneration and allowances decided by the Governor in Council.
- (4) The commissioner is entitled to the leave of absence decided by the Governor in Council.

## **79 Vacancy in office**

The office of the commissioner becomes vacant if the commissioner—

- (a) completes a term of office and is not reappointed; or
- (b) resigns office by signed notice given to the Minister; or
- (c) is removed from office under section 80.

## **80 Removal from office**

- (1) The Governor in Council may remove the commissioner from office if the commissioner—
- (a) has a conviction, other than a spent conviction, for an indictable offence; or
- (b) is an insolvent under administration; or
- (c) is disqualified from managing corporations because of the Corporations Act, part 2D.6.



(2) Also, the Governor in Council may, on the Minister's recommendation, remove the commissioner from office if the Minister is satisfied the commissioner—

- (a) has engaged in—
  - (i) paid employment outside of the commissioner's duties without the Minister's approval; or
  - (ii) inappropriate or improper conduct in an official capacity; or
  - (iii) inappropriate or improper conduct in a private capacity that reflects seriously and adversely on the office; or
- (b) has become incapable of performing the commissioner's functions; or
- (c) has neglected the commissioner's duties or performed the commissioner's functions incompetently.

(3) In this section—

***insolvent under administration*** see the *Corporations Act 2001* (Cwlth), section 9.

***spent conviction*** means a conviction—

- (a) for which the rehabilitation period under the *Criminal Law (Rehabilitation of Offenders) Act 1986* has expired under that Act; and
- (b) that is not revived as prescribed by section 11 of that Act.

## **81 Preservation of rights of public service employee appointed as commissioner**

- (1) This section applies to a person appointed as the commissioner who was a public service employee immediately before taking up the appointment.

DRAFT

[s 82]

---

- (2) The person is entitled to retain all accrued or accruing rights as if service as the commissioner were a continuation of the person's service as a public service employee.

## **82 Preservation of rights of commissioner appointed as public service employee**

- (1) This section applies to a person appointed as a public service employee who was the commissioner immediately before taking up the appointment.
- (2) The person's service as commissioner must be regarded as service as a public service employee.

## **Division 3 Staff of the commission**

### **83 Staff**

- (1) The staff of the commission are employed under the *Public Service Act 2008*.
- (2) The staff of the commission are not subject to direction by anyone other than the commissioner, or a person authorised by the commissioner, about how the commissioner's functions are to be performed.

## **Division 4 Reporting requirements**

### **84 Annual report**

- (1) As soon as practicable after the end of each financial year, the commissioner must give the Minister a report (an ***annual report***) about the operation of this Act during the year.
- (2) Without limiting subsection (1), the report must include information for the financial year about the following matters—

- (a) the number of complaints made or referred to the commissioner;
  - (b) the types of complaints made or referred to the commissioner, including—
    - (i) the categories of entities to which the complaints relate; and
    - (ii) the uses of surveillance devices to which the complaints relate; and
    - (iii) the provisions of part 3 to which the complaints relate;
  - (c) the outcome of complaints made or referred to the commissioner, including—
    - (i) the number of complaints the commissioner refused to deal with, or to continue to deal with, and the grounds for refusing; and
    - (ii) the number and type of complaints referred to another entity under section 51; and
    - (iii) the number and type of complaints resolved by the commissioner by mediation; and
    - (iv) the number and type of complaints referred to QCAT under section 62;
  - (d) the outcome of complaints referred to QCAT;
  - (e) another matter prescribed by regulation.
- (3) The Minister must table a copy of the annual report in the Legislative Assembly within 14 sitting days after receiving the report.

## **85 Other reports**

- (1) The commissioner may prepare a report about a matter relevant to the performance of the commissioner's functions under this Act and give the report to the Minister.

DRAFT

[s 86]

---

- (2) The commissioner must, if asked by the Minister, prepare a report about a matter mentioned in subsection (1) and give the report to the Minister as soon as practicable after it is prepared.
- (3) The Minister must table a copy of a report given to the Minister under subsection (1) or (2) in the Legislative Assembly within 14 sitting days after receiving the report.

## **86 Report containing personal information**

- (1) A report prepared under this division must not include personal information about an individual unless the individual—
  - (a) has previously published the information; or
  - (b) gave the information for the purpose of publication.
- (2) In this section—

*personal information* see the *Information Privacy Act 2009*, section 12.

## **87 Report containing adverse comment**

- (1) This section applies if the commissioner proposes to make an adverse comment about a person in a report prepared under this division.
- (2) The commissioner must give the person an opportunity to respond, in writing, to the proposed adverse comment.
- (3) If the person gives the commissioner a response to the proposed adverse comment and the commissioner still proposes to make the comment, the commissioner must ensure the person's response is fairly stated in the report.
- (4) For this section, an adverse comment does not include a statement that a person did not participate in resolving a surveillance device complaint.

---

## Part 6 Protections

### 88 Protection of commissioner from civil liability

- (1) The commissioner is not civilly liable to someone for an act done, or omission made, under this Act honestly and without negligence.

*Note—*

For protection from civil liability in relation to State employees—see the *Public Service Act 2008*, section 26C.

- (2) If subsection (1) prevents a civil liability attaching to the commissioner, the liability attaches instead to the State.

### 89 Protection of other persons from civil, criminal and administrative liability

- (1) This section applies if a person, acting honestly—
  - (a) gives information to the commissioner under this Act; or
  - (b) gives the commissioner a written response to a complaint under part 4, division 3, or a proposed adverse comment under section 87.
- (2) The person is not liable civilly, criminally or under an administrative process because the person gave the information or written response to the commissioner.
- (3) Also, because the person gave the information or written response to the commissioner, the person can not be held to have—
  - (a) breached any code of professional etiquette or ethics; or
  - (b) departed from accepted standards of professional conduct.

### 90 No communication of official information to court

- (1) This section applies in relation to a person—

DRAFT

[s 91]

---

- (a) who is, or has been, the commissioner or a staff member of the commission; and
- (b) who, in that capacity, acquires, or has access to or custody of, information related to the performance of the person's functions under this Act.
- (2) The person can not be required to give the information to a court.
- (3) Subsection (2) does not apply if the information is given—
  - (a) in performing a function under this Act; or
  - (b) as required or permitted under another Act.
- (4) In this section—
 

**court** includes any tribunal, authority or person having power to require the production of documents or the answering of questions.

**give**, to a court, includes—

  - (a) produce in the court; and
  - (b) permit the court access to.

## Part 7 Offences

### 91 Confidentiality

- (1) This section applies to a person—
  - (a) who is, or has been, the commissioner or a staff member of the commission; and
  - (b) who, in that capacity, acquires or has access to or custody of confidential information.
- (2) However, this section does not apply in relation to information to which section 56 or 90 applies.
- (3) The person must not make a record of the information or disclose the information to another person.

- 
- (4) Subsection (3) does not apply if the record is made or the information is disclosed—
- (a) with the consent of each person to whom the record or information relates; or
  - (b) in performing a function under this Act; or
  - (c) as required or permitted under another Act.
- (5) In this section—

***confidential information***—

- (a) means any information that—
  - (i) relates to a surveillance device complaint, including personal information about the complainant or respondent to the complaint; or
  - (ii) is personal information about another individual; or
  - (iii) is about a person's current financial position or financial background; or
  - (iv) if disclosed, would be likely to damage the commercial activities of a person to whom the information relates; but
- (b) does not include—
  - (i) information that is publicly available; or
  - (ii) statistical or other information that is not likely to result in the identification of a person to whom the information relates.

***personal information*** see the *Information Privacy Act 2009*, section 12.

**92 False or misleading information**

- (1) A person must not, in relation to the administration of this Act, give information that the person knows is false or

DRAFT

[s 93]

---

misleading in a material particular to the commissioner or a staff member of the commission.

Maximum penalty—10 penalty units.

- (2) Subsection (1) applies whether or not the information was given in response to a specific power under this Act.
- (3) Subsection (1) does not apply to information if the person, when giving the information—
  - (a) tells the recipient of the information how it is false or misleading, to the best of the person's ability; and
  - (b) if the person has, or can reasonably obtain, the correct information, gives the correct information.

## Part 8 General

### 93 Delegations

- (1) The commissioner may delegate the commissioner's functions under this Act or another Act to an appropriately qualified staff member of the commission.
- (2) In this section—  
*functions* includes powers.

### 94 Regulation-making power

- (1) The Governor in Council may make regulations under this Act.
- (2) A regulation may—
  - (a) prescribe fees payable under the Act; and
  - (b) provide for a maximum penalty of 20 penalty units for a contravention of a regulation.



**95 Review of Act**

- (1) The Minister must complete a review of the effectiveness of this Act within 5 years after the commencement.
- (2) In completing the review, the Minister must consider—
  - (a) whether this Act is achieving its purpose; and
  - (b) how surveillance devices and surveillance device technologies are used in civil society; and
  - (c) developments in surveillance device technology; and
  - (d) whether the Act should be amended to provide for—
    - (i) new types of surveillance devices; or
    - (ii) new uses of surveillance devices and surveillance device technologies in civil society.
- (3) The Minister must table in the Legislative Assembly a report on the outcome of the review as soon as practicable after the review is completed.

**Part 9 Repeal**

**96 Repeal**

The Invasion of Privacy Act 1971, No. 50 is repealed.

**Part 10 Transitional provision for  
repeal of Invasion of Privacy  
Act 1971**

**97 Proceedings for offences**

- (1) This section applies in relation to an offence against section 43(1) or (5), 44(1), 45(1) or 46(4) of the repealed *Invasion of*

DRAFT

[s 97]

---

*Privacy Act 1971* committed by a person before the commencement.

- (2) Without limiting the *Acts Interpretation Act 1954*, section 20, a proceeding for the offence may be continued or started, and the person may be convicted of and punished for the offence, as if the *Surveillance Devices Act 2020*, section 96 had not commenced.
- (3) Subsection (2) applies despite the Criminal Code, section 11.

DRAFT

---

## Schedule 1      Dictionary

### section 5

**commission** means the Surveillance Devices Commission established under section 66(2).

**commissioner** means the Surveillance Devices Commissioner.

**complainant**, for a surveillance device complaint, means the individual who is the subject of the alleged contravention of section 36 or 37 to which the complaint relates.

**complaint** means a surveillance device complaint.

**computer** means an electronic device for storing and processing information.

**consent** means express or implied consent.

**data surveillance device** see section 10.

**device** includes an instrument, apparatus and equipment.

**general obligation** means an obligation under section 36 or 37.

**health ombudsman** means the health ombudsman under the *Health Ombudsman Act 2013*.

**human rights commissioner** means the commissioner under the *Anti-Discrimination Act 1991*.

**information** includes—

- (a) a record in any form; and
- (b) a document.

**information commissioner** means the information commissioner under the *Right to Information Act 2009*.

**listening device** see section 7.

**maintain**, in relation to a surveillance device, includes—

- (a) adjust, relocate, repair or service the device; and

DRAFT

(b) replace a faulty device.

**notice** means written notice.

**ombudsman** means the ombudsman under the *Ombudsman Act 2001*.

**optical surveillance device** see section 8.

**party**—

(a) to a private conversation—see section 13(1); or

(b) to a private activity—see section 13(2).

**private activity** see section 12.

**private conversation** see section 11.

**proceeding**, in relation to QCAT, see the QCAT Act, schedule 3, definition *proceeding*, paragraph (a).

**purpose of this Act** means the purpose stated in section 2.

**reasonable expectation**, of surveillance privacy for an individual, for part 3, see section 34.

**referral Act** means—

(a) the *Health Ombudsman Act 2013*; or

(b) the *Human Rights Act 2019*; or

(c) the *Information Privacy Act 2009*; or

(d) the *Ombudsman Act 2001*.

**referral entity** means—

(a) the health ombudsman; or

(b) the human rights commissioner; or

(c) the information commissioner; or

(d) the ombudsman.

**respondent**, for a surveillance device complaint, means each person who, under the complaint, is alleged to have contravened section 36 or 37.

**surveillance device** see section 6.

**surveillance device complaint** see section 39.

*surveillance information* see section 14.

*surveillance privacy*, of an individual, for part 3, see section 34.

*tracking device* see section 9.

DRAFT