

Department of Justice and Attorney-General

## Civil surveillance reforms

April 2023



Queensland  
Government



The Queensland Government is committed to providing accessible services to Queenslanders from all culturally and linguistically diverse backgrounds. If you have difficulty understanding this consultation paper, you can contact us on 13 QGOV (13 74 68) and we will arrange an interpreter to effectively communicate the paper to you. If you require assistance in accessing and/or reading this consultation paper, you can also contact us on 13 QGOV (13 74 68).

© State of Queensland (Department of Justice and Attorney-General) 2023. Copyright protects this publication. Excerpts may be reproduced with acknowledgement of the State of Queensland (Department of Justice and Attorney-General). The information contained in this document is subject to change without notice. The Queensland Government shall not be liable for technical or other errors or omissions in this document. The reader/user accepts all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this information.

# Attorney-General's Foreword



Surveillance device technology and the way we use it is constantly evolving both in Queensland and around the world. Community concern over the use of such technology is also growing and it's crucial that we have legislation which keeps pace with these changes, reflects community attitudes and protects the right to privacy.

In Queensland, the regulation of surveillance and surveillance devices is generally less comprehensive than in many other Australian jurisdictions. Currently, the *Invasion of Privacy Act 1971* regulates the use of listening devices in limited circumstances only.

It is understood that all other States and Territories, with the exception of Tasmania and the Australian Capital Territory, have replaced their listening devices legislation with surveillance device legislation. This has enabled the regulation of a wider range of surveillance devices, including listening devices, optical surveillance devices, tracking devices and in some cases, data surveillance devices.

More comprehensive laws are needed to tackle the increasing pitfalls of the surveillance era.

That's why the Palaszczuk Government asked the Queensland Law Reform Commission (QLRC) to review Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies in 2018.

In 2020, the QLRC released its [report](#)<sup>1</sup> on the review, recommending that the *Invasion of Privacy Act 1971* be repealed and replaced by the draft Surveillance Devices Bill (the QLRC draft Bill) which would:

- impose criminal prohibitions and penalties on the use, installation and maintenance of surveillance devices ('use prohibitions') without consent, subject to certain exceptions;
- impose criminal prohibitions and penalties on the communication, or publication of, information obtained from a surveillance device ('communication or publication prohibitions') without consent, subject to certain exceptions;

---

<sup>1</sup> [https://www.qlrc.qld.gov.au/\\_\\_data/assets/pdf\\_file/0003/653322/QLRC-Report-77-online.pdf](https://www.qlrc.qld.gov.au/__data/assets/pdf_file/0003/653322/QLRC-Report-77-online.pdf).

- impose a civil law obligation on a user of a surveillance device not to use the device in a way that interferes with an individual's surveillance privacy if the individual has a reasonable expectation of surveillance privacy and has not consented to the use;
- create a civil mechanism to resolve complaints about, and provide remedies for, an alleged contravention of the above general obligations, based on the model for privacy complaints under the *Information Privacy Act 2009*; and
- establish a Surveillance Devices Commissioner, and a Surveillance Devices Commission, which will receive and deal with complaints.

The Palaszczuk Government is seeking feedback on a staged approach to considering implementation of the reforms recommended by the QLRC, commencing with a legislative scheme for the criminal prohibitions in the QLRC draft Bill to bring Queensland more into line with other States and Territories.

Prohibitions would also be an important measure to combat technology-facilitated domestic and family violence by criminalising surveillance conduct which would amount to serious stalking and coercive control. The proposed reforms would better reflect contemporary tactics used by perpetrators, including electronic or digital monitoring, surveillance on mobile phones, tracking devices on vehicles and the installation of covert cameras.

The Consultation Paper seeks community views on a staged approach to considering implementation of the civil surveillance reforms recommended by the QLRC. It also seeks feedback on the workability of those aspects of the QLRC draft Bill that impose the use prohibitions and communication or publication prohibitions.

I invite everyone to contribute to these important issues by making a submission and look forward to having their feedback.

## **SHANNON FENTIMAN MP**

**Attorney-General and Minister for Justice, Minister for Women and Minister for the Prevention of Domestic and Family Violence**

**April 2023**

# Table of Contents

<b>1. INTRODUCTION</b>	<b>7</b>
1.1. Purpose of this paper	7
1.2. Request for feedback	7
<b>2. BACKGROUND</b>	<b>8</b>
2.1 What is civil surveillance?	8
2.2 Current legislative context in Queensland	9
2.3 Commonwealth surveillance laws	10
2.4 Commonwealth Privacy Act Review Report	10
2.5 Surveillance device legislation in other jurisdictions	11
2.6 Reference to the Queensland Law Reform Commission	11
2.7 Civil surveillance report outcomes	12
2.8 Staged approach to reform	13
2.9 Workplace surveillance	13
<b>3. ISSUES</b>	<b>14</b>
3.1 Regulated categories of surveillance devices	14
3.2 Diagram A – Regulated categories of surveillance devices	15
3.3 Preliminary matters	16
3.4 Criminal prohibitions on use of surveillance devices ('use prohibitions')	18
3.5 Criminal prohibitions on the communication or publication of surveillance information ('communication or publication prohibitions')	26
3.6 Exceptions to the use prohibitions	27
3.7 Exceptions to the communication or publication prohibitions	36
3.8 Other issues	41
3.9 Workplace surveillance	44
3.10 Appendix A: Regulated Categories of Surveillance Device – Listening Device	46
3.11 Appendix B: Regulated Categories of Surveillance Device – Optical Surveillance Device	47
3.12 Appendix C: Regulated Categories of Surveillance Device – Tracking Device	47
3.13 Appendix D: Regulated Categories of Surveillance Device – Data Surveillance Device	49

## Abbreviations

Abbreviation	Definition
<b>ACCC</b>	Australian Competition and Consumer Commission
<b>ACCC Report</b>	Australian Competition and Consumer Commission's report, <i>Digital Platforms Inquiry – Final Report</i>
<b>AIC</b>	Australian Information Commissioner
<b>ALRC</b>	Australian Law Reform Commission
<b>APPs</b>	Australian Privacy Principles
<b>CCC</b>	Crime and Corruption Commission
<b>DFV</b>	Domestic and family violence
<b>DJAG</b>	Department of Justice and Attorney-General
<b>QLRC draft Bill</b>	Draft Surveillance Devices Bill
<b>IoP Act</b>	<i>Invasion of Privacy Act 1971</i>
<b>QDS</b>	Queensland Drones Strategy
<b>QLRC</b>	Queensland Law Reform Commission
<b>QLRC Report</b>	<i>Report No. 77- Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies</i>
<b>VLRC</b>	Victorian Law Reform Commission

# 1. INTRODUCTION

## 1.1. Purpose of this paper

The Queensland Government is considering the recommendations made by the Queensland Law Reform Commission (QLRC) in its *Report No. 77 - Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (QLRC report)<sup>2</sup>, which was tabled on 29 June 2020.

One of the recommendations in the QLRC report is that the *Invasion of Privacy Act 1971* be repealed and replaced by the draft Surveillance Devices Bill (QLRC draft Bill).

The purpose of this consultation paper is to seek feedback on:

- a staged approach to considering implementation of the civil surveillance reforms outlined in the QLRC report; and
- those aspects of the QLRC draft Bill that impose the use prohibitions and communication or publication prohibitions with respect to surveillance devices; and
- whether Queensland should introduce legislation to specifically regulate surveillance in a workplace context to ensure an appropriate balance between the interests of employers and employees.

While it is not intended to explore alternative approaches to the regulation of surveillance devices as recommended by the QLRC, it is important to test the workability of the criminal law aspects of the QLRC draft Bill to determine whether any changes or additional provisions are required to support its effective potential implementation.

## 1.2. Request for feedback

Stakeholder views are sought on the proposals raised in this consultation paper. Stakeholders are requested to provide their feedback on the consultation paper to Strategic Policy, Department of Justice and Attorney-General (DJAG) at [CivilSurveillanceReforms@justice.qld.gov.au](mailto:CivilSurveillanceReforms@justice.qld.gov.au) by **Wednesday 31 May 2023**.

**Personal information** in your comments or submission will be collected by the Department of Justice and Attorney-General (DJAG) for the purpose of informing the civil surveillance reforms in Queensland. DJAG may contact you for further information on the issues you raise. Your comments or submission may also be provided to others with an interest in the reforms, for example, Parliament's Legal Affairs and Safety Committee. Comments and submissions in relation to this consultation paper may be published on DJAG's website. If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly. Please note however that all submissions may be subject to disclosure under the *Right to Information Act 2009*.

---

<sup>2</sup> [https://www.qlrc.qld.gov.au/\\_\\_data/assets/pdf\\_file/0003/653322/QLRC-Report-77-online.pdf](https://www.qlrc.qld.gov.au/__data/assets/pdf_file/0003/653322/QLRC-Report-77-online.pdf).

## 2. BACKGROUND

### 2.1 What is civil surveillance?

‘Surveillance’ generally means ‘watching over’ a person. Surveillance may be overt, covert, or a combination of both. It may occur on a single occasion or be systematic. 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.

Community attitudes about privacy and surveillance are complex. There are many public benefits to be obtained from surveillance activities, and surveillance is used for a wide range 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 crime deterrence.

However, members of the community are becoming increasingly concerned about the use of surveillance devices in a range of contexts as well as the use of a range of new technologies to conduct surveillance. This includes the use by individuals of CCTV cameras directed into their neighbour’s properties, the use by individuals, government agencies and corporations of recreational and commercial drones with advanced optical and audio recording capacity, and the use a range of workplace surveillance devices to monitor employees.

It is also possible for surveillance device technologies to be used to perpetrate domestic and family violence (DFV) or for other 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. As noted by the Women’s Safety and Justice Taskforce (Taskforce) in *Hear her voice: Report one – Addressing coercive control and domestic and family violence in Queensland (First Report)*, coercive control is a pattern of deliberate behaviours, or a course of conduct, used strategically by a perpetrator to exert power and control of another person and creates a one-sided power dynamic in an intimate relationship. The behaviour may include technology-facilitated surveillance of a victim using GPS devices, spyware and mobile phone applications as well as cameras and microphones in victims’ homes and vehicles to track their movements. Technology can also be abused to stalk, intimidate, impersonate, humiliate, threaten or harass victims.

Surveillance devices are constantly evolving, and over time have become more sophisticated, more accessible and more affordable. Their capacity to impact on individuals’ privacy grows as the devices develop and become more widely available.

**Protection from surveillance is a fundamental form of privacy protection.** Article 17 of the International Covenant on Civil and Political Rights relevantly provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.



## 2.2 Current legislative context in Queensland

In Queensland, the regulation of surveillance and surveillance devices is generally less comprehensive than in many other Australian jurisdictions.

The *Invasion of Privacy Act 1971* (IoP Act) only regulates the use of listening devices to the extent that they are used in relation to private conversations. Under the IoP Act, it is an offence for a person using a listening device to overhear, record, monitor or listen to a private conversation ('use prohibition'), unless that person is also a party to the conversation or another exception applies. There are also prohibitions on communicating or publishing information ('communication or publication prohibitions'). There are exceptions to both of the prohibitions, including: if the communication is with the consent of a party to the conversation; or, for the use prohibition, where it is authorised under another law (i.e. use by a police officer or officer of the Commonwealth under another law).

Both the *Police Powers and Responsibilities Act 2000* (chapter 13) and the *Surveillance Devices Act 2004* (Cth) establish procedures for law enforcement officers to obtain warrants and authorities to use a surveillance device in limited circumstances in criminal investigations and other emergency situations. They also restrict the use, communication or publication of information obtained through a surveillance device.

Other Queensland laws only offer piecemeal and limited protection for the privacy of individuals in this context, including the:

- *Information Privacy Act 2009* – which governs the way Queensland government agencies collect, store, use and disclose personal information, but does not regulate surveillance activities by private individuals;
- *Criminal Code* – section 227A makes it an offence to observe or visually record another person in a place where a reasonable adult would expect to be afforded privacy and that place is a private place (e.g. a bathroom). Sections 223 and 229A make it an offence to distribute an intimate image of another person without consent in a way that would cause the other person distress; or threaten to distribute an intimate image of another person without the other person's consent and in a way that would cause a reasonable person distress and to fear the threat would be carried out;
- *Human Rights Act 2019* – which makes it unlawful to act or make a decision in a way that is incompatible with human rights, including the right to privacy (only applies to actions of public entities); and
- common law – including actions in trespass where there is an intrusion onto property; liability in nuisance for interference with the quiet enjoyment of land; breach of confidence which can protect against the misuse or disclosure of 'confidential information'.

The QLRC's proposed criminal prohibitions would complement the reforms proposed by the Taskforce in its First Report to combat technology-facilitated DFV abuse by criminalising surveillance conduct which would constitute an act of stalking (i.e. installing tracking and spyware applications on mobile phones, electronic devices and vehicles as well as installing covert cameras). In response to the recommendations in the Taskforce's First Report, section 359B of the Criminal Code (What is unlawful stalking) has been amended by the (yet to be commenced) *Domestic and Family Violence Protection (Combating Coercive Control) and Other Legislation Amendment Act 2023* to broaden the type of offending captured by the offence and better reflect the way an offender might use technology to facilitate unlawful stalking, intimidation, harassment or abuse. In response to another recommendation made by the Taskforce, the Government has committed to introducing legislation by the end of 2023 to create a new offence to criminalise coercive control.

## 2.3 Commonwealth surveillance laws

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 or permits another person to intercept such a communication, or to do any act or thing that enables the person or another person to intercept such a communication.

The *Telecommunications Act 1997* (Cth) requires carriers, carriage service providers, operators of emergency call services and operators of a public number database to protect the confidentiality of information or documents that relate to:

- the contents or substance of communications carried by carriers or carriage service providers;
- carriage services supplied by carriers or carriage service providers; and
- the affairs or personal particulars (including any unlisted telephone number or any address) of other persons.

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).

## 2.4 Commonwealth Privacy Act Review Report

On 16 February 2023, the Commonwealth Attorney-General publicly released the *Privacy Act Review Report* (Privacy Act Review Report). Proposal 27.1 of the Privacy Act Review Report is to introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in its 2014 Report 123, *Serious Invasions of Privacy in the Digital Era* (ALRC Report) The proposed statutory tort would apply to invasions of privacy by any means and as such would be much broader than the particular context of surveillance devices legislation.

If adopted as per the ALRC Report recommendations, the statutory tort would be enacted in federal legislation to address the current gap in mechanisms available to Australians to seek compensation in the courts for breaches of privacy which fall outside current legislative regimes (including the *Commonwealth Privacy Act 1988* which regulates how Australian Government agencies and organisations with an annual turnover of more than \$3 million, and some other organisations, handle personal information) and state and territory privacy legislation. Action would be able to be commenced in both federal and state and territory courts through cross vesting of federal jurisdiction and courts may have variable associated litigation costs and variable jurisdictional limits to hear claims above certain amounts.

Submissions on the Privacy Act Review Report were due on 31 March 2023 and will inform the Commonwealth Government's response to the report. Timeframes for implementation of reforms are unknown at this stage.

## 2.5 Surveillance device legislation in other jurisdictions

It is understood that all other States and Territories, with the exception of Tasmania and the Australian Capital Territory (ACT),<sup>3</sup> have replaced their listening devices legislation with surveillance device legislation regulating a wider range of surveillance devices including listening devices, optical surveillance devices, tracking devices and in some cases, data surveillance devices.<sup>4</sup>

The ACT, New South Wales (NSW) and Victoria have legislated to specifically regulate workplace surveillance through the *Workplace Privacy Act 2011* (ACT), the *Workplace Surveillance Act 2005* (NSW) and the *Surveillance Devices Act 1999* (Vic), respectively.

The surveillance devices legislation in each jurisdiction includes a prohibition for communicating or publishing surveillance information. All jurisdictions include exceptions to this prohibition, including where there has been consent of all parties to the private communication or activity. Exceptions to the prohibitions vary between jurisdictions.

## 2.6 Reference to the Queensland Law Reform Commission

On 20 July 2018, the QLRC was asked to review Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies; and workplace surveillance.

The terms of reference for the civil surveillance review required the QLRC to recommend whether Queensland should consider legislation to appropriately protect the privacy of individuals in the context of civil surveillance technologies, including to:

- regulate the use of surveillance devices (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;
- regulate the communication or publication of information derived from surveillance devices;
- provide for offences relating to the unlawful use of surveillance devices and the unlawful communication or publication of information derived from a surveillance device;
- provide appropriate regulatory powers and enforcement mechanisms in relation to the use of surveillance devices;
- provide appropriate penalties and remedies; and
- otherwise appropriately protect the privacy of individuals in relation to the use of surveillance devices.

---

<sup>3</sup> *Listening Devices Act 1991* (Tas); *Listening Devices Regulations 2014* (Tas); *Listening Devices Act 1992* (ACT).

<sup>4</sup> *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Regulation 2022* (NSW); *Surveillance Devices Act 2007* (NT); *Surveillance Devices Regulations 2008* (NT); *Surveillance Devices Act 2016* (SA); *Surveillance Devices Regulations 2017* (SA); *Listening Devices Act 1991* (Tas); *Listening Devices Regulations 2014* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Regulations 2016* (Vic); *Surveillance Devices Act 1998* (WA); *Surveillance Devices Regulations 1999* (WA).

The terms of reference excluded Queensland's existing laws regulating the use of surveillance devices for State law enforcement purposes.

The QLRC received 47 written submissions from government agencies and non-government organisations and individuals in response to a public consultation paper it released in December 2018. Agencies including the Queensland Police Service, Office of Fair Trading and Commonwealth Civil Aviation Security Agency provided information about surveillance technologies and practices to the QLRC review.

## 2.7 Civil surveillance report outcomes

As noted in section 1.1, the QLRC report was tabled in the Legislative Assembly on 29 June 2020.

In relation to civil surveillance, the QLRC concluded that there is a need for a more comprehensive legislative response to protect the privacy of individuals and address 'gaps and uncertainties' in relation to the use of surveillance devices in civil society in Queensland. It recommended that the IoP Act be repealed and replaced by the draft Surveillance Devices Bill 2020 (QLRC draft Bill) accompanying the civil surveillance report which encompasses the recommendations in legislative form.

The QLRC draft Bill aims to protect the privacy of individuals from unjustified interference from the use of surveillance devices, or the communication or publication of information obtained from using surveillance devices by, among other things:

- imposing criminal prohibitions on the use, installation and maintenance of surveillance devices, subject to exceptions ('use prohibitions');
- imposing criminal prohibitions on the communication, or publication of, information obtained from a surveillance device, subject to exceptions ('communication and publication prohibitions');
- imposing a civil law obligation on a user of a surveillance device not to use the device in a way that interferes with an individual's surveillance privacy if the individual has a reasonable expectation of surveillance privacy and has not consented to the use;
- creating a civil mechanism to resolve complaints about, and provide remedies for, an alleged contravention of the above general obligations; and
- establishing a Surveillance Devices Commissioner, and a Surveillance Devices Commission, to receive and deal with complaints.

The regulation of the use of surveillance devices under the QLRC draft Bill is based on different principles and policy settings from the IoP Act. In particular, the QLRC draft Bill does not retain participant monitoring, in the absence of consent. That is the QLRC draft Bill generally does not allow the use of a surveillance device by a party to a private conversation (or private activity) without the knowledge or consent of the other party or parties. Instead, in the absence of consent, the use of a surveillance device is generally unlawful unless an exception (for a specific purpose which justifies the use of the device) applies.

## 2.8 Staged approach to reform

In Queensland and (it is understood to be the case) in other States and Territories, the current model for surveillance legislation relies only on criminal prohibitions. The QLRC draft Bill goes further than other states and territories by:

- imposing a civil law 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;
- providing a civil mechanism to resolve complaints about an alleged contravention of a general obligation; and
- establishing a new body to receive and deal with complaints, with a referral power to the Queensland Civil and Administrative Tribunal (QCAT) to hear and determine complaints which are unresolved after mediation.

The Government is seeking feedback on taking **a staged approach to considering implementing the reforms** in the QLRC draft Bill, starting with repealing the IoP Act and implementing the criminal prohibitions in the QLRC draft Bill.

## 2.9 Workplace surveillance

Surveillance devices may be used in workplaces by employers for a number of legitimate reasons, including to protect property and detect possible fraud, to monitor employee performance and to safeguard employee health and safety. For example, optical surveillance devices may be used to monitor in and around workplaces and data surveillance devices may be used to monitor computer and internet use by employees.

While employers in Queensland are required to comply with general laws in respect of surveillance devices, such as the IoP Act and section 227A of the Criminal Code (discussed above at section 2.2), surveillance of employees by employers is not specifically regulated in Queensland.

As noted above in section 2.6, workplace surveillance is the subject of a separate referral to the QLRC. This notwithstanding the Government, as part of this Consultation Paper, is seeking stakeholder views as to whether Queensland should introduce legislation to specifically regulate surveillance in a workplace context to ensure an appropriate balance between the interests of employers and employees. Consideration may need to be given to prohibiting the use of surveillance devices in workplaces without sufficient notice being provided to employees and to protecting the privacy of employees outside of work.

## 3. ISSUES

### 3.1 Regulated categories of surveillance devices

Consistent with surveillance devices legislation in other Australian jurisdictions, the QLRC draft Bill adopts a ‘recognised categories’ approach to regulating surveillance devices – that is, to regulate recognised categories of surveillance devices by reference to the general function or capability of the device. This approach takes into account that different types of devices give rise to different privacy concerns and considerations.

The QLRC draft Bill applies to a wider range of surveillance devices than the IoP Act which, as noted above, only applies to listening devices. Clause 6 of the QLRC draft Bill defines a *surveillance device* to include the following devices:

- a listening device (for example, a bugging device) - a device capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation. However, a listening device does not include a hearing aid or similar device used by an individual with impaired hearing (clause 7);
- an optical device (for example, a camera, video camera or drone) - a device capable of being used to observe monitor or visually record an activity. However, an optical device does not include spectacles, contact lenses or a similar device used by an individual with impaired vision (clause 8);
- a tracking device (for example, a GPS logger or a smart phone with GPS capability) – a device capable of being used to find, monitor or record the geographical location of an individual, vehicle or other thing (clause 9); or
- a data surveillance device (for example, a keylogger) - a device or program capable of being used to access, monitor, or record information that is being input into, output from, or stored in a computer (clause 10) (Computer is further defined to as an electronic device for storing and processing information (Schedule 1 Dictionary).

See **Diagram A** and **Appendix A to D – Regulated Categories of Surveillance Devices**.

It is important that the definition of ‘*surveillance device*’ is clear so that any legislation is enforceable. It is also desirable to aim for as much consistency as possible with definitions in other States and Territories.

## 3.2 Diagram A – Regulated categories of surveillance devices

### (1) Is the surveillance device regulated?

#### Regulated categories of surveillance device

- *Listening device* – capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation
- *Optical surveillance device* – capable of being used to observe, monitor or visually record an activity
- *Tracking device* – capable of being used to find, monitor or record the geographical location of an individual, vehicle or thing
- *Data surveillance device* - device or program capable of being used to access, monitor, or record information that is being input into, output from, or stored in a computer
- A regulated surveillance device also includes a device that is a combination of two or more of those devices listed above.

### (2) Does a criminal prohibition apply to the regulated category of surveillance device?

#### 'Use' criminal prohibitions

These prohibit the use, installation or maintenance of a:

- *listening device* to listen to, monitor or record a private conversation;
- *optical surveillance device* to observe, monitor or visually record a private activity, without the consent of each party to the activity;
- *tracking device* to find, monitor or record the geographical location of an individual, vehicle or other thing; or
- *data surveillance device* to access, monitor or record information that is input into, output from or stored in a computer.

#### 'Communication or publication' criminal prohibitions

These prohibit a person communicating or publishing surveillance information obtained from the use of a surveillance device about:

- a *private conversation* or a *private activity*;
- the *geographical location of an individual, a vehicle or another thing*; or
- *information that is input into, output from or stored in a computer*.

These prohibitions apply if the person knows, or ought reasonably to know, that the information is surveillance information.

### (3) If consent has not been obtained for the use or communication or publication, does an exception apply?

#### 'Use' exceptions

In the circumstances, the use of the surveillance device justifies the interference with privacy:

- where the use is necessary to protect a person's *lawful interests*;
- where the use is reasonably necessary in the *public interest*;
- to obtain evidence or information about a *serious threat to individuals or property*;
- to locate a *stolen vehicle or other thing*; or
- where the use is *otherwise authorised* by an Act or Regulation.

#### 'Communication or publication' exceptions

In the circumstances, the communication or publication of the surveillance information justifies the interference with privacy where it is:

- in a *legal proceeding*;
- reasonably necessary to protect a person's *lawful interests*;
- reasonably necessary in the *public interest*;
- reasonably necessary to lessen/prevent a serious threat to the life, health, *safety* or *wellbeing* of an individual or substantial damage to property; or
- *otherwise authorised* by an Act or regulation.

## Consultation questions

- |                   |   |
|-------------------|---|
| <b>Question 1</b> | <i>Is the proposed definition of ‘surveillance device’, including the definitions of ‘listening device’, ‘optical surveillance device’, ‘tracking device’ and ‘data surveillance device’, sufficiently clear?</i> |
| <b>Question 2</b> | <i>Are there any other types of surveillance devices which should be included in the definition of ‘surveillance device’?</i>   |

### 3.3 Preliminary matters

#### Other laws regulating surveillance devices (clause 4)

The QLRC draft Bill is not intended to affect the operation of another law regulating the use of surveillance devices. In Queensland, in addition to the IoP Act there are other Acts that separately regulate the use of one or more categories of surveillance devices for specific purposes, including law enforcement purposes. For example, the *Police Powers and Responsibilities Act 2000* (PPRA) establishes procedures for police to obtain a warrant or emergency 16authorization for the use of a listening device or a data surveillance device in the criminal investigation of a relevant offence. The *Fisheries Act 1994* authorises an inspector to use a body-worn camera to record images or sounds while exercising a power under the Act.

The QLRC draft Bill provides that it does not affect:

- the operation of another law regulating the use of surveillance devices (e.g. PPRA, chapter 13 or the *Crime and Corruption Act 2001*, chapter 3, part 6); or
- the power of a court to make a decision about the admissibility of information obtained using a surveillance device as evidence in a proceeding.

## Consultation questions

- |                   |  |
|-------------------|--|
| <b>Question 3</b> | <i>Do you have any comments on the relationship between the QLRC draft bill and other laws regulating the use of surveillance devices?</i> |
|-------------------|--|

### Consent

As will be discussed below in further detail, the starting point in the QLRC draft Bill is that the use of a surveillance device is generally unlawful in the absence of consent.

Each of the use prohibitions in the QLRC draft Bill includes a lack of consent as an element of the offence, rather than including consent as an exception to the offence. A person who uses a surveillance device with consent will not commit an offence.



The use of a surveillance device with consent is generally permitted by surveillance devices legislation in other jurisdictions.<sup>5</sup>

Consent is defined in the QLRC draft Bill to mean express or implied consent. In the QLRC's view, the requirements for consent (namely, that the 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. This approach is consistent with surveillance devices legislation in other jurisdictions, and with the IP Act and the *Privacy Act 1988* (Cth).

As noted in the QLRC report, some children and adults will not be able to give or refuse consent under the QLRC 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.<sup>6</sup>

## Consultation questions

**Question 4** *Is the definition of 'consent' in the QLRC draft Bill appropriate?*

**Question 5** *Is the general law sufficient for dealing with issues of consent by children or adults with impaired decision-making capacity?*

## Criminal excuses

As discussed further below, the offences in the QLRC draft Bill do not contain an element of intention.

The QLRC considered that this was not necessary given the availability of section 23(1)(b) of the Criminal Code as an excuse of general application.<sup>7</sup>

Section 23(1)(b) of the Criminal Code provides that a person is not criminally responsible for an event that:

- (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.

The QLRC considered that applying section 23(1)(b) of the Criminal Code, a person would be excused from criminal responsibility for contravention of a use prohibition under the QLRC 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>5</sup> *Listening Devices Act 1992* (ACT) ss 2 (definition of 'consent'), 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); *Invasion of Privacy Act 1971* (Qld) ss 42(2)(b), 43(2)(a).

<sup>6</sup> Queensland Law Reform Commission (QLRC), *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020)49.

<sup>7</sup> *Criminal Code* (Qld) s 36(1).

The QLRC has suggested that 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.

The mistake of fact excuse under section 24 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. In the example 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.<sup>8</sup>

### 3.4 Criminal prohibitions on use of surveillance devices (‘use prohibitions’)

The QLRC draft Bill prohibits the use of surveillance devices in particular circumstances to protect the privacy of individuals from unjustified interference. Specifically, the QLRC Bill contains four separate use prohibitions, one for each category of surveillance device.

The use prohibitions 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 (clause 18)
- an **optical surveillance device** to observe, monitor or visually record a private activity, without the consent of each party to the activity (clause 19)
- a **tracking device** to find, monitor or record the geographical location of:
  - an individual, without the individual’s consent (clause 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 (clause 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 (clause 21).

Under the QLRC draft Bill, a contravention of a use prohibition is a **criminal offence** with a **maximum penalty of three years imprisonment or 60 penalty units (currently \$8625)**. The current penalty in the IoP Act for the use of a listening device in contravention of the Act is a maximum of two years imprisonment and 40 penalty units (currently \$5750). It is important that the criminal penalties for contravening the use prohibitions are proportionate and reflect the seriousness of the act or intrusion into an individual’s privacy.

---

<sup>8</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 80.

Under the QLRC draft Bill, 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 (currently \$43125)**.

The use prohibitions apply to the **use, installation or maintenance** of a surveillance device. The term *use* is not defined so will be given its ordinary meaning. 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>9</sup> The term *maintain* includes: (a) adjust, relocate, repair or service the device; and (b) replace a faulty device.<sup>10</sup> The QLRC draft Bill provides that 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. The QLRC draft Bill does 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 QLRC considered that, ordinarily, a corporate officer should not be made responsible for acts or omissions over which they had no control.

Other elements of the use prohibitions are discussed further detail below. Importantly, the use prohibitions are also subject to certain exceptions (also discussed in further detail below).

## Consultation questions

**Question 6** *Is the proposed penalty amount for contravention of a use prohibition proportionate?*

**Question 7** *Are the elements of the offences, as discussed above, sufficiently clear?*

## Prohibition relating to listening device (clause 18)

The QLRC draft Bill 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.<sup>11</sup> This means that the use of a listening device is regulated only to the extent that it is used in relation to *a private conversation*.

**Private conversation** is defined in clause 11 of the QLRC draft Bill to mean words spoken by an individual if the words spoken are spoken in circumstances that may reasonably be taken to indicate:

- 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 –

---

<sup>9</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 82.

<sup>10</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 57-58.

<sup>11</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 13.

- 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).

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.

The first limb (a) in the definition of '*private conversation*' is intended to ensure that a communication involving one person only, such as a person dictating private information into a computer, is adequately protected in appropriate circumstances. The second limb is intended to protect private communications that are between two or more people. It 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.

It is understood that all other Australian jurisdictions regulate the use of a listening device and generally prohibit the use of a listening device to listen to a private conversation without consent.

It is important to note that unlike the current approach in the IoP Act, it is not enough that the person recording the private conversation is a party to the conversation (i.e. participant monitoring). Consent to record the private conversation must be obtained by all parties.

#### EXAMPLES – USE OF LISTENING DEVICES

**The following activities are likely to be offences (unless consent is obtained or a relevant exception applies):**

- ✘ Use of a listening device to listen to a conversation between two people in a public park where no one else can overhear them.
- ✘ Use of a listening device to record a conversation taking place in a private home between two people.
- ✘ Use of an audio bug on an ex-partner's phone to record their private conversations.

**The following activities are unlikely to be offences:**

- ✓ Use of a listening device to record a conversation between two people in a crowded restaurant that is loud enough for the people seated next to them to overhear.

### **Consultation questions**

**Question 8** Is the proposed definition of 'private conversation' clear?

## Prohibition relating to optical surveillance device (clause 19)

The QLRC draft Bill provides 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 (clause 19).

**Private activity** is defined in clause 12 of the Bill. 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.

The definition of ‘*private activity*’ is consistent with the definition of ‘*private conversation*’ in the QLRC draft Bill and the approach taken in surveillance devices legislation in other jurisdictions. In SA and Victoria, however, the definitions of ‘*private activity*’ are more restrictive than in the QLRC draft Bill. The SA definition excludes an activity carried on in a public place, or in premises or a vehicle if it can be readily observed from a public place.<sup>12</sup> While the Victorian definition does not include an activity carried on outside a building,<sup>13</sup> the Victorian Law Reform Commission (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>14</sup> It is understood that this recommendation has not yet been implemented.

The use prohibition for an optical surveillance device in the QLRC draft Bill is directed to private activities, which are protected regardless of the location in which they occur. The QLRC’s view was that 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.<sup>15</sup> Additionally, in the QLRC’s view, 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.<sup>16</sup>

---

<sup>12</sup> *Surveillance Devices Act 2016* (SA) s3(1) (definition ‘private activity’).

<sup>13</sup> *Surveillance Devices Act 1999* (Vic) s3(1) (definition ‘private activity’).

<sup>14</sup> Victorian Law Reform Commission (VLRC), *Surveillance in public places* (Report No 18, August 2010), 16.

<sup>15</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 90.

<sup>16</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 90.

## EXAMPLES – USE OF OPTICAL DEVICES

The following activities are likely to be offences (unless consent is obtained or a relevant exception applies):

- ✘ Installing a camera in your ex-partner’s bathroom to watch them shower without their consent.
- ✘ Using a CCTV camera to record activities in your neighbor’s bedroom or bathroom.
- ✘ Using a drone with a camera to record footage of your neighbours in a pool that would otherwise be obscured from public view.

The following activities are unlikely to be offences:

- ✓ Filming a street performer or to taking photographs in the open at a tourist attraction.
- ✓ Using a dashboard-mounted camera whilst driving on a public road.
- ✓ Using binoculars to watch a soccer match being played in a public field.<sup>17</sup>

## Consultation questions

**Question 9** *Is the proposed definition of ‘private activity’ reasonably clear?*

**Question 10** *Should private activities be protected regardless of whether they occur in a public or outdoor place?*

## Prohibition relating to tracking device (clause 20)

The prohibitions in relation to the use of tracking devices in the QLRC draft Bill relates to both:

- individuals; and
- vehicles or other things.

The QLRC 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 consent of the individual (clause 20(1)).

---

<sup>17</sup> Women’s Services Network (WESNET), Legal Guide to Surveillance Legislation in WA, *Technology Safety Australia* (Web Page) <[https://techsafety.org.au/blog/legal\\_articles/legal-guide-to-surveillance-legislation-in-wa/](https://techsafety.org.au/blog/legal_articles/legal-guide-to-surveillance-legislation-in-wa/)>.

Also, 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 (clause 20(2)).

#### EXAMPLES – USE OF TRACKING DEVICES

- ✘ A person cannot put a GPS tracking device into their partner’s handbag without their consent.<sup>18</sup>
- ✓ An employer could install a GPS tracking device in their employee’s company car with consent.

Unlike the regulation of the use of a listening device or an optical surveillance device, which is generally limited in application to a ‘private conversation’ or a ‘private activity’, the regulation of the use of a tracking device applies whether or not the relevant information or location is ‘private’.<sup>19</sup> The QLRC considered that while there was a general acceptance of the everyday use of listening devices and optical devices in public spaces (e.g. taking audio and visual recordings at public events), there are greater expectations of privacy associated with tracking devices.

In relation to tracking vehicles or other things, consent must be provided by each person who owns or is in lawful control of the vehicle or thing.

While the QLRC draft Bill does not define the term ‘lawful control,’ the QLRC Report states that a person who is in ‘lawful control’ of a vehicle or other thing may include a person who:

- 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.<sup>20</sup>

The QLRC acknowledged that in circumstances where a vehicle or other thing is the subject of a lease or hire agreement, it may be unrealistic to expect the owner’s consent each time a person seeks to use, install or maintain a tracking device. Further the person who leases or hires a vehicle or other thing from another person would generally (particularly where there is a long-term arrangement) consider themselves to be in a similar position to an owner for the purpose of giving consent to the use of a tracking device.

Clause 16 of the QLRC draft Bill provides 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:

---

<sup>18</sup> Women’s Services Network (WESNET), Legal Guide to Surveillance Legislation in WA, *Technology Safety Australia* (Web Page) <[https://techsafety.org.au/blog/legal\\_articles/legal-guide-to-surveillance-legislation-in-wa/](https://techsafety.org.au/blog/legal_articles/legal-guide-to-surveillance-legislation-in-wa/)>.

<sup>19</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 92.

<sup>20</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 97.

- (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.

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.<sup>21</sup>

As noted by the QLRC, 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.<sup>22</sup>

NSW, Victoria, SA, Western Australia (WA) and Northern Territory (NT) legislation regulates the use of a tracking device.

## Consultation questions

**Question 11** *Is the proposed definition of 'excluded owner' appropriate?*

**Question 12** *Is it practical to require the consent of each person where there is more than one person who is an owner or a person in lawful control?*

**Question 13** *Is it clear who would be in 'lawful control' of a vehicle or thing?*

## Prohibition relating to data surveillance device (clause 21)

The QLRC draft Bill provides 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.<sup>23</sup> Like tracking devices, the regulation of the use of a data surveillance device applies whether or not the relevant information or location is 'private'.<sup>24</sup>

---

<sup>21</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 98.

<sup>22</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 98.

<sup>23</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 14.

<sup>24</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 92.



A **computer** means an electronic device for storing and processing information.

The focus is on obtaining the consent of the owner, or person in lawful control of the computer. The QLRC acknowledged that a person who experiences interference with their privacy due to the use of a data surveillance device may not be the owner or the person in control of a computer, such as at an internet café or a public library.<sup>25</sup> The QLRC considered it may be impractical and onerous to identify and obtain the consent of each person who uses a public computer.

Consistent with the approach to tracking devices, a reference to a person who ‘owns’ a computer excludes 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 (an excluded owner).

Also consistent with the approach in relation to tracking devices, consent must be provided by each person who owns or is in lawful control of the computer.

The QLRC draft Bill does not define ‘lawful control’ in relation to the use of data surveillance devices. In NSW and SA, 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 without the owner’s consent or the consent of the person in lawful control of the computer.<sup>26</sup> 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 the NT 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>27</sup> In the NT, this also applies to officers from the Independent Commission Against Corruption. Surveillance device legislation in WA does not regulate data surveillance devices.<sup>28</sup>

#### EXAMPLES – USE OF DATA SURVEILLANCE DEVICES

**The following activities are likely to be offences (unless consent is obtained or a relevant exception applies):**

- ✘ Installing spyware on another person’s smartphone or tablet to monitor their digital activity (such as phone calls, social media activity, calendar entries, text messages and website browser history) without their consent.

**The following activities are unlikely to be offences**

- ✓ The owner of an internet café installing a keylogger on the computers in the café.

<sup>25</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 99.

<sup>26</sup> *Surveillance Devices Act 2007* (NSW) s 10(1); *Surveillance Devices Act 2016* (SA) s 8(1).

<sup>27</sup> *Surveillance Devices Act* (NT) s 14(1); *Surveillance Devices Act 1999* (Vic) s 9(1).

<sup>28</sup> *Surveillance Devices Act 1998* (WA).

Some parents or schools may use a data surveillance device, such as internet monitoring software, to monitor their children's mobile phone or computer activity. Whether the use will be an offence under the QLRC draft Bill will depend on a number of factors including whether consent for the use has been obtained. Whether a child has capacity to give or refuse consent to the use will depend on the particular circumstances of the case.

## **Consultation questions**

**Question 14** *Is it practical to require the consent of each person where there is more than one person who is an owner or a person in lawful control?*

**Question 15** *Is it sufficiently clear who would be in lawful control of a computer?*

### **3.5 Criminal prohibitions on the communication or publication of surveillance information ('communication or publication prohibitions')**

The QLRC draft Bill prohibits a person communicating or publishing surveillance information obtained from the use of a surveillance device without consent.

The QLRC considered that these communication or publication prohibitions provided an important additional protection which recognises the breach of privacy caused by the communication or publication of surveillance information.

Surveillance information is defined in clause 14 of the QLRC draft Bill as 'information obtained, directly or indirectly, using a surveillance device'. The schedule dictionary of the QLRC draft Bill defines 'information' to include a record in any form and a document. This is intended to 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.

Specifically, the QLRC draft Bill contains three separate communication or publishing prohibitions which prohibit a person communicating or publishing surveillance information 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 (clause 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 (clause 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 (clause 30).

Surveillance devices legislation in other jurisdictions generally prohibits the communication or publication of information obtained from the use of a surveillance device, subject to exceptions. 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.<sup>29</sup>

Consistent with the use prohibitions in the QLRC draft Bill, contravention of a communication or publication prohibition is a criminal offence with a **maximum penalty of three years imprisonment or 60 penalty units (currently \$8625)**.

## Consultation questions

**Question 16** *Is the proposed penalty amount for contravention of a communication or publication prohibition proportionate?*

### 3.6 Exceptions to the use prohibitions

The QLRC 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. Each exception applies to each category of surveillance device. As noted by the QLRC, generally the exceptions are drafted in broad terms and their application will depend on the facts and circumstances of a particular matter. In some instances, the use of a surveillance device may fall within the scope of multiple exceptions.

**Exceptions to the use prohibitions** include:

- where the use is necessary to protect a person's **lawful interests** (clause 22);
- where the use is reasonably necessary in the **public interest** (clause 23);
- to obtain evidence or information about a **serious threat** (clause 24);
- to **locate a stolen vehicle** (clause 25); and
- where the use is otherwise **authorised under another Act** or in circumstances prescribed by Regulation (clause 26).

---

<sup>29</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.

## Protection of lawful interests (clause 22)

Clause 22 of the QLRC draft Bill provides that 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.

The exception provides that (a) 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 to protect their own lawful interests. It also provides that (b) 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 the other person. While the QLRC considered that the law of agency could be used to satisfy limb (b) of the exception, it was included for clarity.

While the term 'lawful interests' is not defined in the QLRC Bill or other surveillance devices legislation, it has been the subject of judicial consideration.

In *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd*,<sup>30</sup> Doyle J considered that the concept of 'lawful interests' is of 'uncertain content' and the issue of whether a recording was made for the protection of a person's lawful interests is anchored in the facts of the particular case. In relation to what would not give rise to a lawful interest, Doyle J commented 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 to protect a person's lawful interests;<sup>31</sup> and
- 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 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.<sup>32</sup>

In contrast, Doyle J commented 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.<sup>33</sup>

---

<sup>30</sup> *Nanosecond Corporation Pty Ltd & Anor v Glen Carron Pty Ltd & Anor* (2018) 132 SASR 63, [101].

<sup>31</sup> *Nanosecond Corporation Pty Ltd & Anor v Glen Carron Pty Ltd & Anor* (2018) 132 SASR 63, [103].

<sup>32</sup> *Nanosecond Corporation Pty Ltd & Anor v Glen Carron Pty Ltd & Anor* (2018) 132 SASR 63, [104].

<sup>33</sup> *Nanosecond Corporation Pty Ltd & Anor v Glen Carron Pty Ltd & Anor* (2018) 132 SASR 63, [105].

## EXAMPLES

Other circumstances in which a person has been found to have used a surveillance device in a way that protected their lawful interests include:<sup>34</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.

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>35</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 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>34</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>35</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].

In *Sepulveda v R*, the NSW Court of Appeal interpreted the exception narrowly in finding that it was not reasonably necessary for a sexual assault victim to secretly record the perpetrator admitting to the assault. This was because the victim could have approached the police with his complaints.<sup>36</sup>

The QLRC considered it beneficial that there is scope for the concept of lawful interests to be considered on the facts of each case.<sup>37</sup>

The QLRC draft Bill limits the lawful interests exception by requiring that the use is 'reasonably necessary' and 'to protect' a person's lawful interests. The QLRC considered that the incorporation of reasonableness as an objective test is important so that it operates in appropriate circumstances.<sup>38</sup>

Similar exceptions exist in legislation in NSW, ACT, SA and Tasmania and WA. The term 'lawful interests' is not defined in these jurisdictions. In these jurisdictions the exception operates as a limited form of participant monitoring. A party to a conversation may record a private conversation or activity if it is reasonably necessary to protect the principal party's lawful interests. As a result, the recording may be made by a principal party without the consent of others. In South Australia, this exception also extends to protecting the lawful interests of the person who uses the device.

## Consultation questions

**Question 17** *Would the term lawful interests be sufficiently understood by persons seeking to comply with or enforce the QLRC draft Bill so as to be readily applied as an exception?*

**Question 18** *It is necessary for the exception to apply to the lawful interests of other people in limb (b) above given the common law doctrine of agency?*

## Reasonably necessary in the public interest (clause 23)

Clause 23(1) of the QLRC draft Bill provides that 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.

To provide guidance about the circumstances in which using a device might be reasonably necessary in the public interest, the QLRC draft Bill includes a list of relevant matters to provide a framework for courts and persons in determining whether the use of a surveillance device is reasonably necessary in the public interest in particular circumstances.<sup>39</sup>

---

<sup>36</sup> *Sepulveda v R* [2006] NSWCCA 379, [139].

<sup>37</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 108.

<sup>38</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 108.

<sup>39</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 277.

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.

The QLRC noted that 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>40</sup>

## EXAMPLES

Examples of matters that might, depending on the circumstances, be 'in the public interest' include:

- ✓ the prevention and detection of illegal activities, for example, the investigation of a crime or detection of insurance fraud;
- ✓ public office 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.<sup>41</sup>

---

<sup>40</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 116.

<sup>41</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 111.

The QLRC considered that the term ‘public interest’ should not be defined because an understanding of ‘public interest’ is generally contextual and what is in the public interest also changes over time.<sup>42</sup>

Conversely, in WA and the NT, the term ‘public interest’ is defined by surveillance devices legislation 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.*<sup>43</sup>

The term ‘public interest’ is not defined in SA’s surveillance device legislation. NSW and Victoria do not have a public interest exception.

## Consultation questions

**Question 19** *Is the term ‘in the public interest’ sufficiently clear so as to be readily applied as an exception?*

**Question 20** *Should the term ‘reasonably necessary in the public interest’ be further defined?*

**Question 21** *Are the considerations for deciding whether the use of a surveillance device is reasonably necessary in the public interest necessary and appropriate?*

## Evidence of serious threat to individuals or property (clause 24)

Clause 24 of the QLRC draft Bill provides 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 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 (clause 24(1)).

A **serious threat** is defined to mean:

- (a) a serious threat to the life, health or wellbeing of an individual; or
- (b) a serious threat of substantial damage to property.<sup>44</sup>

This approach is intended to make clear that a person can use a surveillance device to obtain evidence or information in appropriate circumstances, but places a limit on the use of a surveillance device by including the requirement of immediacy. It requires that a threat be in existence at the time that a surveillance device is used and a belief that it is necessary to use the device immediately (for example, a person is not able use other appropriate means such as reporting their concerns to the police).

---

<sup>42</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 115.

<sup>43</sup> *Surveillance Devices Act* (NT) s 41; *Surveillance Devices Act 1998* (WA) s 24 (definition of ‘public interest’).

<sup>44</sup> QLRC, *Review of Queensland’s laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 16.



Tasmania includes a similarly styled exception which 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>45</sup>

In WA, 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, such as where the use will contribute towards the protection of the best interests of the child or protected person and is in the public interest.<sup>46</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>47</sup> Surveillance device legislation in NSW, SA and Victoria does not have an exception in connection with safety and wellbeing.

## Consultation questions

**Question 22** *Is the exception for evidence of a serious threat to individuals or property sufficiently clear?*

### Locate lost or stolen vehicle or other thing (clause 25)

Clause 25 of the QLRC draft Bill provides that 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.

The concept of lawful control is discussed above under the use prohibitions.

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. It does not allow a person to use a surveillance device to locate or retrieve a vehicle or other thing if the person was not, prior to it being lost or stolen, an owner or person in lawful control of it.

#### EXAMPLE

- ✓ A person who has attached a tracking device to their stolen bicycle could use that device to find its location.

---

<sup>45</sup> Tasmania, Parliamentary Debates, Legislative Assembly (1 May 1991) 934–5 (PJ Patmore, Minister for Justice).

<sup>46</sup> *Surveillance Devices Act 1998* (WA) ss 5(2)(d), 6(2)(d), 26(3), 27(3).

<sup>47</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).

This exception is broader in NSW and SA where it is not an offence for a person to use a listening device, an optical surveillance device or (in SA) a tracking device, if it is used solely for the purposes of locating and retrieving that device.<sup>48</sup> In WA, it is not an offence for a person to use a tracking device in relation to an object that:

- (a) was in the person's possession or under the person's control when the device was attached or installed;
- (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.<sup>49</sup>

## Consultation questions

**Question 23** *Is it appropriate to have an exception for the purpose of location and/or retrieval of a vehicle or thing?*

## Otherwise authorised (clause 26)

Clause 26 of the QLRC draft Bill provides that a person who uses, installs or maintains a surveillance device does not commit an offence against section 18, 19, 20 or 21 (the use prohibitions) 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.

This exception is intended to ensure that use of a surveillance device that is expressly authorised by another Act is not affected.

### EXAMPLES

Some examples of authorising Acts include:

- ✓ the PPRA, which regulates the use of a surveillance device by police officers in certain circumstances and authorises the use of a body-worn camera by police officers;<sup>50</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>51</sup>

---

<sup>48</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).

<sup>49</sup> *Surveillance Devices Act 1998* (WA) s 7(2)(d); *Surveillance Devices Regulations 1999* (WA) reg 6(2).

<sup>50</sup> *Police Powers and Responsibilities Act 2000* (Qld) ch 13, s 609A.

<sup>51</sup> *Youth Justice Act 1992* (Qld) s 263A(1), (2), (6).

- ✓ the *Fisheries Act 1994*, which authorises the use of a body-worn camera by inspectors and the use of vessel tracking equipment by relevant boats;<sup>52</sup>
- ✓ 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>53</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>54</sup>

The QLRC did not consider that the exception should be broad enough to cover instances where a surveillance device *might* be used to satisfy a requirement to monitor something without specifying how that monitoring should be carried out (for example, the *Food Production (Safety) Regulation 2014* which provides that Safe Food Production Queensland may monitor compliance with food safety schemes).<sup>55</sup> However, the QLRC noted that 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>56</sup>

The QLRC 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 intended to provide some flexibility, while the requirement for this to be prescribed through regulation provides for an appropriate degree of oversight.

## Consultation questions

**Question 24** *Is the exception for lawful authorization sufficiently clear?*

**Question 25** *When, if at all, would it be appropriate to prescribe by regulation additional circumstances in which the use, installation or maintenance of a surveillance device without consent is not an offence?*

<sup>52</sup> *Fisheries Act 1994* (Qld) ss 80, 181A(4).

<sup>53</sup> *Bail Act 1980* (Qld) s 11(9B).

<sup>54</sup> *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.

<sup>55</sup> *Food Production (Safety) Regulation 2014* (Qld), sch 13, s 45.

<sup>56</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 125-126.

### 3.7 Exceptions to the communication or publication prohibitions

The QLRC draft Bill also includes a number of exceptions to the communication or publication prohibitions under which it is not an offence to communicate or publish surveillance information, without consent, in circumstances where the interference with privacy is justified.

**Exceptions to the communication or publication prohibitions** include where the communication or publication of surveillance information without consent is:

- in a legal proceeding;
- reasonably necessary to protect a person's lawful interests;
- 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.

#### Communication or publication in legal proceedings (clause 31(a))

Clause 31(1)(a) of the QRLC Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is in a legal proceeding.

This exception is intended to apply where surveillance information is communicated or published to a court or tribunal. It is not intended to make the information admissible if it is not otherwise admissible in court proceedings. In that regard, clause 4 of the QRLC Bill clarifies that the Act 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.

All jurisdictions have an exception permitting communication or publication in the course of some or all legal proceedings. The scope of the 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.

Unlike the IoP Act, which defines legal proceeding in section 45 to include proceedings (whether civil or criminal) 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, the QLRC draft Bill does not define the term 'legal proceeding'.

#### Consultation questions

**Question 26** *Should the term 'legal proceeding' be defined in the QRLC Bill?*

## Communication or publication to protect a person's lawful interests (clause 31(b))

Clause 31(1)(b) of the QLRC draft Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is reasonably necessary to protect the lawful interests of:

- (a) the person; or
- (b) another person who has authorised the person to communicate or publish the information on the other person's behalf.

This exception is intended to apply 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. It is also intended to apply to protect the lawful interests of another person who has authorised the person to communicate or publish the information on the other person's behalf.

### EXAMPLE

- ✓ In the QLRC's view, the communication or publication of surveillance information by private investigators or loss adjusters would be adequately covered by the exceptions included in the QLRC draft Bill, including the exception for communication or publication of surveillance information where it is reasonably necessary to protect a person's lawful interests or in the public interest (discussed below).

Similar exceptions exist in the ACT, NT, Tasmania, Victoria, SA and WA. For example, in the ACT and WA, a person does not commit an offence if the person's communication or publication of surveillance information is done to protect the lawful interests of a principal party, in circumstances where the device is used with the consent of a principal party to protect their lawful interests. In SA, the exception extends to a media organisation where a device is used in the public interest to protect a lawful interest.

As discussed above, the term 'lawful interests' is not defined in the QLRC draft Bill or in surveillance devices legislation in other States and Territories. A person's lawful interests are to be determined on the particular facts of the case. As with the lawful interests exception for the use prohibitions, the communication or publication must be 'reasonably necessary' to protect the person's lawful interests, which is to be assessed objectively, taking into account the particular circumstances of the case.

## Consultation questions

**Question 27** *Is the exception for publication or communication to protect a person's lawful interests sufficiently clear?*

## Communication or publication in the public interest (clause 31 (c))

Clause 31(1)(c) of the QLRC draft Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is reasonably necessary in the public interest.

Like the public interest exception for the use prohibitions, in deciding whether a person's communication or publication of surveillance information is reasonably necessary in the public interest, a court must consider a number of factors as they existed when the person communicated or published the information. Factors to be considered include:

- (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 reasonably 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.

In relation to paragraph (b) above, the scope of the communication or publication 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>57</sup>

### EXAMPLE

- ✓ In the QLRC's view, the public interest exception will apply to surveillance information communicated or published by media organisations and journalists provided it is reasonably necessary in the public interest.

Surveillance devices legislation in the NT and Victoria 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>58</sup> Surveillance devices legislation in other jurisdictions does not contain a broad exception for communication or publication in the public interest. In SA and WA, 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>59</sup>

---

<sup>57</sup> *Channel Seven Perth Pty Ltd v S* (2007) 34 WAR 325 [40], [54]–[57]; *Australian Broadcasting Corporation v SAAWA Pty Ltd* [2018] WASCA 29 [27]–[28],[76]–[78].

<sup>58</sup> *Surveillance Devices Act* (NT) s 15(2)(b)(i); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(i).

<sup>59</sup> *Surveillance Devices Act 2016* (SA) s 10(1); *Surveillance Devices Act 1998* (WA) s 31.

## Consultation questions

**Question 28** *Is the public interest exception sufficiently clear?*

**Question 29** *Should the term 'public interest' be defined?*

**Question 30** *Are there any additional matters the court should be required to consider in deciding whether a person's communication or publication of surveillance information is reasonably necessary in the public interest?*

## Communication or publication for safety and well-being (clause 31(d))

Clause 31(1)(d) of the QLRC draft Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is reasonably necessary to lessen or prevent a serious threat:

(a) to the life, health, safety or wellbeing of an individual; or

(b) of substantial damage to property.

This exception is consistent with the serious threat exception relating to use prohibitions discussed above. NSW, SA, Tasmania and WA have communication or publication exceptions in connection with safety and wellbeing. For example, in South Australia the exception applies where a person is being subjected to violence or there is an imminent threat of violence to a person.

## Consultation questions

**Question 31** *Should there be a safety and wellbeing exception in relation to the communication and publication of surveillance information?*

## Communication or publication authorised under another Act or prescribed by regulation (clause 31(e) and (f))

Clause 31(1)(e) of the QLRC draft Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is authorised under another Act of the State or an Act of the Commonwealth.

Clause 31(1)(f) of the QLRC draft Bill provides that a person does not commit an offence against section 28, 29 or 30 if the person's communication or publication of surveillance information is in circumstances prescribed by regulation for the subsection.

Where communication or publication is authorised under another Act, the person making the communication or publication must comply with any requirements under the Act authorising the use, communication or publication.

This exception should cover the communication or publication of surveillance information by public officers in the course of performing their statutory functions where it is authorised under an Act.

This exception is consistent with exceptions in ACT, NT, SA, Tasmania and Victoria.

Clause 31(1)(f) is intended to enable additional circumstances to be prescribed by regulation and is consistent with the approach taken in relation to the use prohibitions.

In the QLRC's view, 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.<sup>60</sup>

## Consultation questions

**Question 32** *When, if at all, would it be appropriate to prescribe by regulation additional circumstances in which it is not an offence to communicate or publish surveillance information without consent?*

**Question 33** *Government departments are asked to consider their own legislation and whether it requires amendments to expressly authorise the communication or publication of surveillance information in particular circumstances.*

## Law enforcement purposes

The QLRC draft Bill does not include specific exceptions for the use of surveillance devices, without consent, by police or other public officers for State law enforcement purposes. As noted above at section 2.6, the terms of reference for the civil surveillance review excluded Queensland's existing laws regulating the use of surveillance devices for State law enforcement purposes.

As noted in the QLRC Report, police officers are assisted in their activities by recordings made outside the scope of the *Police Powers and Responsibilities Act 2000* by individuals using surveillance devices. Under the IoP Act, it is currently lawful for a person who is a party to a private conversation to use a listening device to record the conversation, without the other party's consent. A person who was the victim of or a witness to a criminal offence might, for example, 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.

As noted above at section 2.7, the QLRC draft Bill does not retain participant monitoring in the absence of consent, but instead includes a number of general purpose-based exceptions outlined above. This will have an impact on the circumstances in which a listening device, or other surveillance device, may be used by an individual or law enforcement officer without consent to provide information or evidence to assist with police investigations.

---

<sup>60</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 166.



## Consultation questions

**Question 34** *Do you think that the exceptions in the QLRC draft Bill adequately ensure that surveillance activities conducted for law enforcement and related purposes can continue to be undertaken? Otherwise, should there be a specific exception for law enforcement related purposes and if so, in what circumstances should it apply?*

### 3.8 Other issues

#### Possessing surveillance information (clause 27)

Clause 27(1) of the QLRC 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 section 18, 19, 20 or 21 (the use prohibitions).

*Relevant person* is defined in clause 27(3) to mean:

- (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.

Clause 27(2) of the QLRC draft Bill provides that a person does not commit an offence against 27(1) if the person:

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

The purpose of the prohibition against possessing surveillance information is to reduce the risk of unlawfully obtained surveillance information being communicated or published.<sup>61</sup>

Contravention of the possessing surveillance information prohibition in the QLRC draft Bill is a criminal offence with a maximum penalty of one year's imprisonment or 20 penalty units (currently \$2875).

Surveillance devices legislation in the Australian Capital Territory, Tasmania, New South Wales and Western Australia includes provisions that make it an offence to possess records obtained from the prohibited use of a surveillance device. In each of these jurisdictions, the offence does not apply if the record is in the possession of the person in connection with proceedings for an offence against the legislation, with the consent of each principal party to the private conversation (or each party 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.

## Consultation questions

**Question 35** *Is the proposed penalty amount for contravention of the possessing surveillance information offence proportionate?*

## Non-publication orders (clause 32)

In its report, the QLRC noted 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. Publication in a court proceeding of information which has been obtained in contravention of the QLRC draft Bill's protections can operate in some circumstances to further the unjustified interference.

On this basis, clause 32(2) and (3) of the QLRC draft Bill provides that if the court considers it is necessary in the interests of justice, the court may make a non-publication order prohibiting the publication of evidence given before the court. Clause 32(4) provides that the court may make a non-publication order at any time during the proceeding.

Contravention of a non-publication order is a criminal offence, unless the person has a reasonable excuse, with a maximum penalty of three years imprisonment or 60 penalty units (currently \$8625).

The provision in the QLRC draft Bill to empower the making of a non-publication order continues the approach taken under section 46(3) of the IoP Act in relation to criminal offences under that Act.

Similar provision, although varying in terms and scope, is made in the surveillance devices legislation in the ACT and Tasmania.

---

<sup>61</sup> QLRC, *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (Report No 77, February 2020) 175.

## Consultation questions

**Question 36** *Is the proposed penalty amount for contravention of a non-publication order proportionate?*

**Question 37** *Is the power for the court to make a non-publication order necessary or desirable?*

### Court may order forfeiture or destruction (clause 33)

The QLRC considered that the court should have the power to order forfeiture of a surveillance device used in connection with the commission of an offence under the Act. The QLRC also considered that the court should have the power to order the forfeiture of other relevant devices or things, such as a USB device on which the record is stored, in addition to the power to order the forfeiture or destruction of any original or copy of the record.

Accordingly, clause 33 of the QLRC draft Bill provides that if a person is convicted of an offence against the Act, the court before which the person is convicted may make an order that:

- (a) a surveillance device used in connection with the commission for 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.

Clause 33(7) defines 'related information' to mean, for an offence: information to which the offence relates; or information obtained using a surveillance device to which the offence relates.

Clause 33 further 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.

Currently, the IoP Act provides for the forfeiture of a listening device used in breach of the Act.

With the exception of Victoria, the surveillance devices legislation in other Australian States and Territories also provides for the court to make forfeiture orders upon conviction for an offence. In some jurisdictions like the NT, the court may also order the forfeiture or destruction of the record made by the device.

## Consultation questions

**Question 38** *Given that devices such as computers and smartphones may be used in contexts that fall outside the scope of the QLRC draft Bill, should the court have the power to order forfeiture of a surveillance device used in connection with the commission of an offence under the Act?*

**Question 39** *Are any additional safeguards required in relation to the forfeiture order power?*

## 3.9 Workplace surveillance

### Limitations with the criminal prohibitions in the QLRC draft Bill

The criminal prohibitions in the QLRC draft Bill are of general application and, if enacted, would apply to all persons and workplaces and their surveillance device practices. In practice, however, the criminal prohibitions in the QLRC draft Bill may have limited application in the workplace.

For example, the criminal prohibitions will not apply to the use of surveillance devices where the person consents to the use of the surveillance device. However, the concept of consent in the workplace is problematic given the general power imbalance between employers and employees. The criminal prohibitions in the QLRC draft Bill will offer no protection to employees who agree to employer use of surveillance devices in circumstances where they may not feel they are free to withhold their consent.

Also, the offences in the QLRC draft Bill in relation to listening devices and optical devices only apply where the conversations and activities being monitored ought reasonably to be expected to be private (due to the definitions of “private conversation” and “private activity”). Consequently, in most workplace contexts, the criminal prohibitions in the QLRC draft Bill may not offer full protection to employees against surveillance in the workplace.

### Workplace surveillance legislation in other jurisdictions

As noted above in section 2.5, the ACT, NSW and Victoria have legislated to specifically regulate workplace surveillance through the *Workplace Privacy Act 2011* (ACT), the *Workplace Surveillance Act 2005* (NSW) and the *Surveillance Devices Act 1999* (Vic), respectively. In these jurisdictions, employers must comply with both specific workplace surveillance legislation and general surveillance device legislation, which applies more broadly than in the workplace, including to surveillance undertaken by individuals and private organisations.<sup>62</sup>

In the ACT, the *Workplace Privacy Act 2011* (ACT) applies to optical devices, tracking devices and data surveillance devices, but not to listening devices. An employer must provide particular forms of notice to

---

<sup>62</sup> Note that ACT’s surveillance device legislation, the *Listening Devices Act 1992* (ACT), only regulates listening devices.

employees if one of these types of surveillance devices is in use in the workplace and must consult with employees in good faith before surveillance is introduced.

The *Workplace Privacy Act 2011* (ACT) also provides for 'covert surveillance authorities', allowing an employer to conduct covert surveillance (surveillance that takes place without the awareness of employees) without providing notice upon receiving an authority from a court (a covert surveillance authority). A covert surveillance authority can be issued only for the purpose of determining whether an employee is carrying out an unlawful activity and is subject to various safeguards.

Surveillance of employees in places such as toilets, change rooms, nursing rooms, first-aid rooms and prayer rooms, and surveillance of employees outside the workplace is also prohibited.

In NSW, the *Workplace Surveillance Act 2005* (NSW) applies to camera surveillance, computer surveillance and tracking surveillance. Surveillance devices must not be used in a workplace without sufficient notice being provided to employees. For camera surveillance, cameras must be visible and there must be signs notifying people they are under camera surveillance. For computer surveillance, surveillance must be carried out in accordance with a policy of the employer on computer surveillance of employees at work and the employee must have been notified in advance about the policy. For tracking surveillance, there must be a notice or visible warning (clearly visible on the thing that is subject to tracking (for example, a vehicle)) that puts the employee on notice that they are under tracking surveillance.

Similar to the ACT, there are also specific areas of a workplace that cannot be monitored, including toilets, changing rooms and shower facilities. Surveillance must also not be used to conduct surveillance of the employee outside work.

In NSW, covert surveillance must not be used unless a covert surveillance authority is obtained from a Magistrate.

In Victoria, part 2A of the *Surveillance Devices Act 1999* (Vic) expressly prohibits employers from using optical surveillance devices or listening devices to observe, listen to, record or monitor the activities or conversations of a worker in a toilet, washroom, change room or lactation room in the workplace. Part 2A also prohibits employers from knowingly communicating or publishing a record or report of an activity or conversation observed, listened to, recorded or monitored by the use of an optical surveillance device or a listening device.

## **Consultation questions**

**Question 40** *Should Queensland legislation specifically regulate the surveillance of employees by employers using surveillance devices (such as optical surveillance devices, tracking devices, listening devices and data surveillance devices)? If so, which types of devices should be regulated and in what circumstances?*

**Question 41** *If so, should Queensland legislation establish particular notice requirements in relation to the use of surveillance devices in workplaces?*

### 3.10 Appendix A: Regulated Categories of Surveillance Device – Listening Device

(1) Is the device a *listening device*?

- A *listening device* is capable of being used to listen to, monitor or record words spoken to, or by, an individual in a conversation.
- It does not include a hearing aid or similar device used by an individual with impaired hearing.

(2) Does a *criminal prohibition* apply to the listening device?

#### 'Use' criminal prohibition

The use, installation or maintenance of a *listening device* to listen to, monitor or record a *private conversation* is prohibited.

#### 'Communication or publication' criminal prohibition

The communication or publication of surveillance information obtained from the use of a *listening device* about a *private conversation* is prohibited.

This prohibition applies if the person knows, or ought reasonably to know, that the information is surveillance information.

(3) Is the conversation a *private conversation*?

#### Private conversation

Words if spoken in circumstances that may reasonably be taken to indicate:

- (a) the individual does not want anyone else to listen to the words (for words not spoken to anyone else); or
- (b) the individual (or at least one 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; or (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 (i) and (ii) to listen to the conversation.

Does not include words spoken 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.

(4) If the conversation is a *private conversation* and consent has not been obtained for the use or communication or publication, does an *exception* apply?

#### 'Use' exceptions

In the circumstances, the use of the listening device justifies the interference with privacy:

- where the use is necessary to protect a person's *lawful interests*;
- where the use is reasonably necessary in the *public interest*;
- to obtain evidence or information about a *serious threat to individuals or property*;
- to locate a *stolen vehicle or other thing*; or
- where the use is *otherwise authorised* by an Act or Regulation.

#### 'Communication or publication' exceptions

In the circumstances, the communication or publication of the surveillance information justifies the interference with privacy where it is:

- in a *legal proceeding*;
- reasonably necessary to protect a person's *lawful interests*;
- reasonably necessary in the *public interest*;
- reasonably necessary to lessen/prevent a serious threat to the life, health, *safety or wellbeing* of an individual or substantial damage to property; or
- *otherwise authorised* by an Act or regulation.

### 3.11 Appendix B: Regulated Categories of Surveillance Device – Optical Surveillance Device

(1) Is the device an *optical surveillance device*?

- An *optical surveillance device* is capable of being used to observe, monitor or visually record an activity.
- It does not include spectacles, contact lenses or a similar device used by an individual with impaired vision.

(2) Does a *criminal prohibition* apply to the optical surveillance device?

#### 'Use' criminal prohibition

The use, installation or maintenance of an *optical surveillance device* to observe, monitor or visually record a *private activity* is prohibited.

#### 'Communication or publication' criminal prohibition

The communication or publication of surveillance information obtained from the use of an optical surveillance device about a *private activity* is prohibited.

This prohibition applies if the person knows, or ought reasonably to know, that the information is surveillance information.

(3) Is the activity a *private activity*?

#### Private activity

Activity carried out in circumstances that may reasonably be taken to indicate that:

- (a) the individual does not want anyone else to observe the activity (for an activity carried out by 1 individual); or
- (b) at least one 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.

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.

(4) If the activity is a *private activity* and consent has not been obtained for the use or communication or publication, does an *exception* apply?

#### 'Use' exceptions

In the circumstances, the use of the optical surveillance device justifies the interference with privacy:

- where the use is necessary to protect a person's *lawful interests*;
- where the use is reasonably necessary in the *public interest*;
- to obtain evidence or information about a *serious threat to individuals or property*;
- to locate a *stolen vehicle or other thing*; or
- where the use is *otherwise authorised* by an Act or

#### 'Communication or publication' expectations

In the circumstances, the communication or publication of the surveillance information justifies the interference with privacy where it is:

- in a *legal proceeding*;
- reasonably necessary to protect a person's *lawful interests*;
- reasonably necessary in the *public interest*;
- reasonably necessary to lessen/prevent a serious threat to the life, health, *safety or wellbeing* of an individual or substantial damage to property; or
- *otherwise authorised* by an Act or regulation.

## 3.12 Appendix C: Regulated Categories of Surveillance Device – Tracking Device

(1) Is the device a *tracking device*?

- A *tracking device* is capable of being used to find, monitor or record the geographical location of an individual, vehicle or thing.

(2) Does a *criminal prohibition* apply to the tracking device?

### 'Use' criminal prohibition

The use, installation or maintenance of a *tracking device* to find, monitor or record the *geographical location* of an individual, vehicle or other thing is prohibited.

(3) If consent has not been obtained for the use or communication or publication, does an *exception* apply?

### 'Use' exceptions

In the circumstances, the use of the tracking device justifies the interference with privacy:

- where the use is necessary to protect a person's *lawful interests*;
- where the use is reasonably necessary in the *public interest*;
- to obtain evidence or information about a *serious threat to individuals or property*;
- to locate a *stolen vehicle or other thing*; or
- where the use is *otherwise authorised* by an Act or Regulation.

### 'Communication or publication' criminal prohibition

The communication or publication of surveillance information obtained from the use of a tracking device about a *geographical location* is prohibited.

This prohibition applies if the person knows, or ought reasonably to know, that the information is surveillance information.

### 'Communication or publication' exceptions

In the circumstances, the communication or publication of the surveillance information justifies the interference with privacy where it is:

- in a *legal proceeding*;
- reasonably necessary to protect a person's *lawful interests*;
- reasonably necessary in the *public interest*;
- reasonably necessary to lessen/prevent a serious threat to the life, health, *safety or wellbeing* of an individual or substantial damage to property; or
- *otherwise authorised* by an Act or regulation.



### 3.13 Appendix D: Regulated Categories of Surveillance Device – Data Surveillance Device

(1) Is the device a *data surveillance device*?

- A *data surveillance device* is a device or program capable of being used to access, monitor, or record information that is being input into, output from, or stored in a computer

(2) Does a *criminal prohibition* apply to the data surveillance device?

#### 'Use' criminal prohibition

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 is prohibited.

#### 'Communication or publication' criminal prohibition

The communication or publication of surveillance information obtained from the use of a data surveillance device about information that is input into, output from or stored in a computer is prohibited.

This prohibition applies if the person knows, or ought reasonably to know, that the information is surveillance information.

(3) If consent has not been obtained for the use or communication or publication, does an *exception* apply?

#### 'Use' exceptions

In the circumstances, the use of the data surveillance device justifies the interference with privacy:

- where the use is necessary to protect a person's *lawful interests*;
- where the use is reasonably necessary in the *public interest*;
- to obtain evidence or information about a *serious threat to individuals or property*;
- to locate a *stolen vehicle or other thing*; or
- where the use is *otherwise authorised* by an Act or Regulation.

#### 'Communication or publication' exceptions

In the circumstances, the communication or publication of the surveillance information justifies the interference with privacy where it is:

- in a *legal proceeding*;
- reasonably necessary to protect a person's *lawful interests*;
- reasonably necessary in the *public interest*;
- reasonably necessary to lessen/prevent a serious threat to the life, health, *safety or wellbeing* of an individual or substantial damage to property; or
- *otherwise authorised by an Act or regulation*.