

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN QUEENSLAND

Introduction

Technology-facilitated stalking and abuse is the use of technology (such as the internet, social media, mobile phones, computers, and surveillance devices) to stalk and perpetrate abuse on a person.

Such behaviour includes:

- Making numerous and unwanted calls to a person's mobile phone
- Sending threatening and/or abusive messages (text messaging, WhatsApp, Snapchat, Facebook messaging, Twitter)
- Hacking into a person's email or social media account to discover information about them
- Hacking into a person's email or social media account to impersonate them and send abusive messages to family/friends of that person
- Using surveillance devices to spy on a person
- Using tracking devices to follow a person
- Sharing, or threatening to share, intimate pictures of a person

This legal guide is one of a set of four guides that looks at areas of law relevant to people experiencing technology-facilitated stalking and abuse.

Legal Guide to Surveillance Legislation in QLD

This guide looks at what the law says about surveillance devices – when it is an offence to use them and what the restrictions are on sharing information/videos/pictures obtained through the use of surveillance devices.

For information on other areas of law see:

Legal Guide to Relevant Criminal Offences in QLD

This guide looks at the various criminal offences that may apply to a person who is perpetrating technology-facilitated stalking and abuse.

Legal Guide to Domestic Violence Protection Orders in QLD

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In Queensland these protection orders are called **domestic violence protection orders (DVOs)**.

Legal Guide to Image-Based Abuse Legislation in QLD

This guide looks at what the law says about image-based abuse – when it is an offence to record or distribute intimate images and what legal options exist for victims of image-based abuse.

Language

‘Victim’ vs. ‘Survivor’

Some women who are experiencing, or who have experienced, domestic violence use the term ‘victim’ of domestic violence to describe themselves. Others believe the term ‘survivor’ of domestic violence more accurately reflects their experience. Whilst acknowledging that each woman’s experience is unique and individual to her circumstances, for consistency, these guides will refer to women who are experiencing, or who have experienced, domestic violence as ‘victim-survivors’ of domestic violence.

Gender

While domestic violence can happen in many circumstances, in the vast majority of reported domestic violence cases men are the people perpetrating the abuse and women are the victim-survivors. For this reason these guides use ‘he’ to refer to perpetrators and ‘she’ to refer to victims. This is not intended to exclude other situations.

Terminology

Criminal Offence (or offence)

A criminal offence is an offence against the State. It is commonly referred to as ‘breaking the law’.

Summary offence

Less serious offences (such as parking violations), are known as summary offences. Summary offences normally have a maximum penalty of no more than 12 months imprisonment or are not punishable by imprisonment at all.

Indictable (serious) offence

More serious offences (such as murder, manslaughter, sexual assault) are known as indictable offences. Indictable offences are punishable by imprisonment exceeding 12 months.

Charge

When a person is charged with an offence, it means that the police have formally accused that person of committing an offence.

Conviction

When a person is convicted of an offence, it means that person has either pleaded guilty to committing the offence, or a court has found that person guilty of committing the offence.

Penalty unit

Criminal legislation usually describes the amount payable for a fine in a “penalty unit”. Penalty units are used instead of dollar amounts because the rate for penalty units is indexed for inflation and may change from time to time. The Penalties and Sentences Regulation 2015 (QLD) states the dollar amount for one penalty unit. As of 1 July 2021, one penalty unit = \$137.85. Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of \$6,892.50.

SURVEILLANCE LEGISLATION IN QUEENSLAND

Invasion of Privacy Act 1971 (Qld)

The *Invasion of Privacy Act 1971* (Qld) (the “Act”) regulates the use of the use of listening devices in Queensland. It does not address the regulation of other surveillance devices such as optical surveillance, tracking, and data surveillance devices.

Use of Listening Devices

A ‘listening device’ means any instrument apparatus, equipment or device capable of being used to overhear, record, monitor or listen to a private conversation simultaneously with its taking place. It does not include a reference to a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and to permit the person only to hear sounds ordinarily audible to the human ear.

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

When is it an offence to use a listening device

It is an offence for a person to use a listening device to *overhear, record, monitor or listen* to a private conversation.

There are wide exceptions that apply to this offence. See *When can a listening device be used*, below.

Maximum penalty: 40 penalty units or imprisonment for 2 years.

When can a listening device be used

A ‘party to a private conversation’ may use a listening device to overhear, record, monitor or listen to a private conversation. A party to a private conversation is:

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

This is a wide definition, including persons by or to whom words are spoken (‘principal parties’) as well as any person who, with the express or implied consent, of any of the principal parties, overhears, records, monitors or listens to the private conversation.

Where can I find this information in the Act?

See sections 4, 42 and 43 of the Act.

Sharing of Private Conversations

Sharing of private conversations unlawfully listened to

It is an offence for a person to communicate or publish to any other person a private conversation, or a report of, or of the substance, meaning or purport of, a private conversation, that has come to his or her knowledge as a direct or indirect result of the use of a listening device in contravention of section 43 (see above).

Maximum penalty: 40 penalty units or imprisonment for 2 years.

If a person has unlawfully listened to a private conversation, they may only share knowledge of that conversation

to a party to the conversation or with the express or implied consent of a party to the conversation.

A person may share knowledge of a private conversation if that knowledge was not obtained through the unlawful use of a listening device (e.g. a person overheard a private conversation without use of a listening device).

Sharing of private conversations by parties to that conversation

It is an offence for a person who, having been a party to a private conversation and having used a listening device to overhear, record, monitor or listen to that conversation, to subsequently communicate or publish to any other person any record of the conversation made, directly or indirectly, by the use of the listening device, or any statement prepared from such a record.

Maximum penalty: 40 penalty units or imprisonment for 2 years.

Therefore, a party to a private conversation (whether a principal party or not) who uses a listening device to *overhear, record, monitor or listen* to the conversation may not communicate or publish a record or statement of the conversation made from the use of the listening device. However, there is no bar to a party to a private conversation later telling another person (who is not a party to the private conversation) what was discussed in the private conversation as long as there was no use of a listening device (though other laws might apply in such a situation e.g. breach of confidence).

There are several relevant exceptions to this offence. A party to a private conversation may share that conversation if the communication or publication:

- is made to another party to the private conversation
- is made with the express or implied consent of all other parties to the private conversation by or to whom words are spoken (principal parties)
- is in the public interest (*public interest* is not defined in the Act)
- is not more than reasonably necessary for the protection of the lawful interests of that person
- is made to a person who has, or whom the sharer on reasonable grounds believes has, such an interest in the private conversation as to make the communication or publication reasonable under the circumstances in which it is made.

Where can I find this information in the Act?

See sections 44 and 45 of the Act.

Telecommunications (Interception and Access) Act 1979 (Cth)

The primary purpose of the *Telecommunications (Interception and Access) Act 1979* (Cth) ("TIA Act") is to protect the privacy of individuals who use the Australian telecommunications system.

Intercepting telecommunications

When is it an offence to intercept telecommunications

It is an offence to:

- (a) intercept;
- (b) authorise, suffer or permit another person to intercept; or
- (c) do any act or thing that will enable him or her or another person to intercept;

a communication passing over a telecommunications system.

Exceptions to this offence exist but are related to law enforcement or the installation or maintenance of telecommunication systems by carriers, and are not relevant in the context of domestic violence.

'Communication' includes conversation and a message, and any part of a conversation or message, whether in the form of speech, music or other sounds, data, text, visual images, whether or not animated, signals or in any other form or in any combination of forms.

A communication starts 'passing over' a telecommunications system when it is sent or transmitted by the person sending the communication, and continues until it becomes accessible to the intended recipient of the communication.

A 'telecommunications system' means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both (but does not include a system, or series of systems, for carrying communications solely by means of radio communication) that is

(a) is within Australia; or

(b) partly within Australia, but only to the extent that the network is within Australia;

and includes equipment, a line or other facility that is connected to such a network and is within Australia.

Maximum penalty: Imprisonment for 2 years.

- **For example:** It is an offence for a person to record his partner's phone calls using an app he installs on her phone.

Where can I find this information in the TIA Act?

See sections 7 and 105. See sections 5 and 5F for definitions.

Dealing with intercepted information

When is it an offence to deal with intercepted information

A person must not communicate to another person, make use of, or make a record of, or give evidence in a proceeding any information that has been intercepted (subject to the other provisions of Part 2-6).

Maximum penalty: Imprisonment for 2 years (see section 105).

Where can I find this information in the TIA Act?

See sections 63 and 105.

Gathering evidence to prove technology-facilitated stalking or abuse

Sometimes it can be difficult to prove technology-facilitated stalking or abuse. Some tips for gathering evidence to show that technology-facilitated stalking or abuse has occurred are:

- Do not delete text messages, voicemail messages, photos
- Try and save any evidence to a computer/USB flash drive
- Use screenshots and save the image as the date & time it was taken. If taking screenshots of websites, always include the URL in the screenshot
- Keep a diary or voice notes of incidents including dates and times
- Consider giving police written permission to access your phone, computer, Facebook, email account etc. if a matter is being investigated

Note: certain other conduct in relation to technology-facilitated stalking or abuse may constitute a criminal offence. Please see the ***Legal Guide to Image-based Abuse in QLD*** and the ***Legal Guide to Relevant Criminal Offences in QLD*** for further information.

March 2022