

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN VICTORIA

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 VIC

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 VIC

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 Family Violence Intervention Orders in VIC

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In Victoria these protection orders are called **Family Violence Intervention Order (FVIOs)**.

Legal Guide to Image-Based Abuse Legislation in VIC

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 Department of Treasury and Finance set the dollar amount for one penalty unit; this value is updated on 1 July each year. As of July 2021, one penalty unit = \$181.74.

SURVEILLANCE LEGISLATION IN VICTORIA

Surveillance Devices Act 1999 (Vic)

The *Surveillance Devices Act 1999 (Vic)* (the 'Act') regulates the installation, use, maintenance and retrieval of surveillance devices in Victoria.

A 'surveillance device' means a data surveillance device, a listening device, an optical surveillance device or a tracking device.

A device that combines two or more of the devices above is also considered a surveillance device.

A 'device' includes instruments, apparatus and equipment.

Where can I find this information in the Act?

See section 3 of the Act.

Use of Listening Devices

A 'listening device' means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear.

A 'private conversation' means a conversation carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves. It does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it may be overheard by someone else.

When is it an offence to use a listening device

It is an offence for a person to knowingly *install, use or maintain* a listening device to *overhear, record, monitor or listen* to a private conversation to which the person is not a party without the permission of each party to the conversation.

When can a listening device be used

Other than law enforcement exceptions, a person can only use a listening device to record a private conversation to which he or she is a party.

Maximum penalty: 240 penalty units or imprisonment for 2 years or both.

- **For example:** A man installs an audio bug on his wife's phone to listen to and record her private conversations.

Where can I find this information in the Act?

See sections 3 and 6 of the Act.

Use of Optical Surveillance Devices

An 'optical surveillance device' means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

A 'private activity' means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves. It does not include an activity carried on outside a building or an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else.

When is it an offence to use an optical surveillance device

It is an offence for a person to knowingly install, use or maintain an optical surveillance device to record visually or observe a private activity to which the person is not a party, without the permission of each party to the activity.

Maximum penalty: 240 penalty units or imprisonment for 2 years or both.

- **For example:** A man installs a secret camera in his ex-partner's bathroom to watch her shower.

When can an optical surveillance device be used

Other than law enforcement exceptions, a person can only use an optical surveillance device to:

- record a private activity to which the person is a party
- record any other activity that is not a private activity (e.g. filming a street performer, filming an activity taking place in a front yard or on a house)

Where can I find this information in the Act?

See sections 3 and 7 of the Act.

Use of Tracking Devices

A 'tracking device' means an electronic device the primary purpose of which is to determine the geographical location of a person or an object.

When is it an offence to use a tracking device

It is an offence for a person to knowingly *install, use or maintain* a tracking device to determine the geographical location of a person, without the express or implied consent of that person.

Likewise, it is also an offence for a person to knowingly *install, use or maintain* a tracking device to determine the geographical location of an object, with the express or implied consent of the person who has lawful possession or lawful control of that object.

Maximum penalty: 240 penalty units or imprisonment for 2 years or both.

- **For example:** A man installs a GPS tracking device in his ex-wife's car so he can monitor her movements.

When can a tracking device be used

Other than law enforcement exceptions, tracking device can only be legally used with the consent, expressed or implied, of the person being tracked by the tracking device. Or in the case of an object, if the person who has lawful possession or lawful control of that object has expressly or impliedly consented.

Where can I find this information in the Act?

See sections 3 and 8 of the Act.

Use of Data Surveillance Devices

A 'data surveillance device' means any device capable of being used to record or monitor the input of information into or the output of information from a computer. It does not include an optical surveillance device (i.e. a video camera filming the typing of words on a computer is not a data surveillance device).

The Act only regulates the installation, use and maintenance of data surveillance devices by law enforcement officers; it is silent on the use of data surveillance devices by the general population. However, the unauthorised installation, use, or maintenance of a data surveillance device could potentially be an offence under the *Crimes Act 1958* (Vic) sections 247A to 247I. For further information please see the **Legal Guide to Relevant Criminal Offences in VIC**.

Where can I find this information in the Act?

See sections 3 and 9 of the Act.

Sharing of Private Conversations or Recordings of Activities**When is it an offence to share a private conversation or recordings of activities**

It is an offence for a person to knowingly *communicate or publish* a record or report of a private conversation or private activity that has been made as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device.

Maximum penalty: 240 penalty units or imprisonment for 2 years or both.

- **For example:** If two people consensually film a sexual act in private (not a contravention of the surveillance legislation) and one person later shares it without the consent of the other party, it would be an offence for that person to share it.

When can a private conversation or recordings of activities be shared

There are several exceptions that apply, however. Most relevantly in this context, communication or publication is allowed if it is no more than is reasonably necessary for the *protection of the lawful interests* of the person making it.

Where can I find this information in the Act?

See section 11 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:

- intercept;
- authorise, suffer or permit another person to intercept; or
- 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

- is within Australia; or
- 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 VIC* and the *Legal Guide to Relevant Criminal Offences in VIC* for further information.

March 2022