

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN SOUTH AUSTRALIA

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 SA

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 SA

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 Intervention Orders in SA

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In South Australia these protection orders are called **Intervention Orders (IOs)**.

Legal Guide to Image-Based Abuse in SA

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 disorderly conduct), are known as summary offences. Summary offences are defined by the Summary Procedure Act 1921 (SA) and have a maximum penalty of no more than two years imprisonment or are not punishable by imprisonment at all.

Indictable offence

More serious offences are known as indictable offences. Indictable offences are divided into minor and major indictable offences. Minor indictable offences are less serious (such as stalking) and are usually dealt with in the Magistrates Court. Major indictable offences are the most serious (such as murder, manslaughter, sexual assault) and are dealt with by the District or Supreme Court.

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.

SURVEILLANCE LEGISLATION IN SOUTH AUSTRALIA

Surveillance Devices Act 2016 (SA)

The *Surveillance Devices Act 2016 (SA)* (the 'Act') regulates the use of listening devices, optical surveillance devices, tracking devices and data surveillance devices in South Australia.

It also restricts the communication and publication of information obtained through the use of these devices.

Use of Listening Devices

A *listening device* means a device capable of being used to listen to or record a private conversation or words in a private conversation. A device may be a listening device as well as another kind of surveillance device. It does not include hearing aids or similar.

- **For example:** Handheld devices such as mobile phones and tablets, which have inbuilt audio recording capabilities; voice recorders/dictation equipment, audio bug surveillance devices.

When is it an offence to use a listening device

It is an offence for a person to intentionally use a listening device to knowingly *install, use or cause to be used or maintain* a listening device to *overhear, record, monitor or listen* to a private conversation to which the person is not a party, or to record a private conversation to which the person is a party.

Remember this prohibition is only for *private* conversations. A listening device can be used where the conversation is not private. A "private conversation" means a conversation carried on in circumstances that may reasonably be taken to indicate that at least one party to the conversation desires it to be heard only by the other parties to the conversation. It does not include a conversation made in circumstances in which all parties to the conversation ought reasonably to expect that it may be heard by a person who is not a party to the conversation.

For example:

- A conversation between two people in a crowded food court that is loud enough for the people seated next to them to hear would not be a private conversation
- A conversation between two people at low volume in a busy park where there is no one close to them would be a private conversation
- A conversation between two people taking place in a private home where they are alone would be a private conversation

Maximum penalty: \$15 000 or imprisonment for 3 years.

- **For example:** It is an offence for a person to install an audio bug surveillance device in his home to non-consensually record, monitor, or listen to private conversations his wife has with other people.
 - Note: this activity could also potentially be an 'unlawful stalking' offence under section 19AA, *Criminal Law Consolidation Act 1953 (SA)*. For further information please see the **Legal Guide to Relevant Criminal Offences in SA**.
 - Note: If that person installed a bug on a telephone to intercept and listen to/record both sides of the telephone conversation then it would also be a federal offence under the *Telecommunications (Interception and Access) Act 1979 (Cth)* (see below).

Where can I find this information in the Act?

See sections 3 and 4 of the Act.

When can a listening device be used

There are a number of exceptions to the above offences. The most relevant state that it is not an offence:

- For a party to a private conversation to use a listening device to record the conversation if all parties expressly or impliedly consent to the device being so used
 - For a party to a private conversation to use a listening device to record the conversation if the use of the device is reasonably necessary for the protection of the lawful interests of that person
 - For a person to use a listening device for a specified law enforcement purpose or as otherwise authorised by law
 - For a person to unintentionally hear a private conversation by means of a listening device
 - For a person to use, install or maintain a listening device if the use of the device is in the public interest
- **For example:** A woman makes an audio recording of her ex-partner threatening her in breach of a domestic violence intervention order. It could be said that the use of the device is reasonably necessary to protect her lawful interests.

Where can I find this information in the Act?

See sections 4 and 6 of the Act.

Use of Optical Surveillance Devices

An 'optical surveillance device' means a device capable of being used to observe or record visually (whether for still or moving pictures) a person, place or activity; and associated equipment. It does not include spectacles, contact lenses or similar, and it also does not include telescopes, binoculars of similar.

When is it an offence to use a visual surveillance device

It is an offence for a person to knowingly *install, use or maintain* an optical surveillance device on or in premises, a vehicle or any other thing, (whether or not the person has lawful possession or lawful control of the premises, vehicle or thing) to *record visually or observe* the carrying on of a private activity without the express or implied consent of each party to the activity.

If the installation, use or maintenance of the device involves entry onto or into premises or a vehicle, the express or implied consent of the owner or occupier is also required. If the installation, use or maintenance of the device involves interference with premises, vehicle or thing, the express or implied consent of the person having lawful possession or control of the premises, vehicle or thing is also required.

Maximum penalty: \$15,000 or imprisonment for 3 years.

- **For example:** A man installs a hidden camera in his wife's car so he can monitor whom she drives with.

There are a number of exceptions to the above offences. The most relevant state that it is not an offence:

- For a person to install, use or maintain an optical surveillance device on premises if the use of the device is reasonably necessary for the protection of the lawful interests of that person
 - For a person to use an optical surveillance device for a specified law enforcement purpose or as otherwise authorised by law
 - For a person to use, install or maintain an optical surveillance device if the use of the device is in the public interest
- **For example:** It is not an offence for a person to install security cameras in their home to monitor any break-ins.

Where can I find this information in the Act?

See sections 3, 5 and 6 of the Act.

Use of Tracking Devices

A 'tracking device' means an electronic device capable of being used to determine the geographical location of a person or thing, and associated equipment.

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, or a vehicle or thing without the express or implied consent of the owner, or a person in lawful possession or lawful control, of that vehicle or thing.

Maximum penalty: \$15,000 or imprisonment for 3 years.

- **For example:** A man installs a tracking device in his ex-partner's car without her knowledge to monitor her location.

Exemptions apply to certain uses for specified law enforcement purposes or as otherwise authorised by law.

Where can I find this information in the Act?

See sections 3 and 7 of the Act.

Use of Data Surveillance Devices

A 'data surveillance device' means a program or device capable of being used to access, track, monitor or record the input of information into, or the output of information from, a computer, and associated equipment.

When is it an offence to use a data surveillance device

It is an offence for a person to knowingly install, use or maintain a data surveillance device to access, track, monitor or record the input of information into, the output of information from, or information stored in, a computer without the express or implied consent of the owner, or person with lawful control or management, of the computer.

Maximum penalty: \$15,000 or imprisonment for 3 years.

- **For example:** A man installs an app on his partner's computer that allows him to monitor all of her actions on the computer.

Where can I find this information in the Act?

See sections 3 and 8 of the Act.

Communication or Publication of Information or Material

When is it an offence to communicate or publish information or material

It is an offence for a person to knowingly use, communicate or publish information or material derived from the use (whether by that person or another person) of a surveillance device (listening device, optical surveillance device, tracking device or data surveillance device) in contravention of any of the above offences.

Maximum penalty: \$15,000 or imprisonment for 3 years, or \$10,000 where the information or material was derived from the use of a listening device or an optical surveillance device in circumstances where the device was used in the public interest or to protect the person's lawful interests.

Where can I find this information in the Act?

See sections 3, 9, 10 and 12 of the Act.

When can information or material be communicated

There are a number of exceptions to the above offence. The most relevant state that it is not an offence:

- To communicate or publish information or material to a person who was a party to the conversation or activity to which the information or material relates
- To communicate or publish information or material with the consent of each party to the conversation or activity to which the information or material relates
- To communicate or publish information or material if that information was also obtained in a manner that did not contravene the Act

- To communicate or publish information or material derived from the use of a listening device or an optical surveillance device in circumstances where the device was used to protect the lawful interests of that person in relation to a situation in which a person is being subjected to violence, or there is an imminent threat of violence
- To communicate or publish information or material derived from the use of a listening device or an optical surveillance device in circumstances where the device was used to in the public interest and where the communication or publication was made to a media organisation

Where can I find this information in the Act?

See sections 9, 10, 11 and 12 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 radiocommunication) 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 SA*** and the ***Legal Guide to Relevant Criminal Offences in SA*** for further information.

March 2022