WESTERN AUSTRALIA

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN WESTERN 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 WA

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 WA

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 Restraining Orders in WA

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

Legal Guide to Image-Based Abuse Legislation in WA

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 obscenity or loitering), are known as summary offences. Summary offences are dealt with by the Magistrates Court.

Indictable offence

More serious offences (such as murder, manslaughter, sexual assault) are known as indictable offences. Indictable offences are heard by the District Court or the 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 WESTERN AUSTRALIA

Surveillance Devices Act 1998 (WA)

The *Surveillance Devices Act 1998* (WA) (the 'Act') regulates the use of surveillance devices in Western Australia. It also restricts the communication and publication of information obtained through the use of surveillance devices.

A 'surveillance device' means a listening device, an optical surveillance device or a tracking device. However, there is no mention of data surveillance devices in the legislation.

Note: Time limits apply. Proceedings for an offence under this Act must be commenced within 2 years after the offence was committed.

Where can I find this information in the Act?

See section 3 of the Act for definitions of terms used in the Act and section 38 for the time limit.

Use of Listening Devices

A 'listening device' means any instrument, apparatus, equipment, or other device capable of being used to record, monitor or listen to a private conversation or words spoken to or by any person in private conversation. This does not include a hearing aid 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 to *install*, *use*, *or maintain* a listening device to *record* a private conversation whether or not the person is a party to the conversation.

If a person is not a party to a private conversation it is also an offence for them to install, use, or maintain a listening device to *monitor or listen* to the private conversation.

It is also an offence to *cause* a listening device to be installed, used, or maintained for one of the above purposes. E.g. paying someone to install a device for you.

Remember this prohibition is only for *private* conversations. A listening device can be used where the conversation is not private. Private conversations do not include conversations where those involved should have reasonably expected that the conversation may be overheard.

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 private
- 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: $5,000 or imprisonment for 12 months or both.

➢ **For example:** It is an offence for a person to install an audio bug surveillance device in his home to record, monitor, or listen to private conversations his wife has with other people, for example to listen to what she says in telephone conversations with other people. If that person installed a bug on the 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 5 and 34 of the Act.

When can a listening device be used

It is legal if you *unintentionally hear* a private conversation through a listening device. E.g. if you unintentionally heard a private conversation between two people coming from a baby monitor which was left on in a separate room of a house.

It is legal to record a private conversation to which you are a party if all of the principal parties to that conversation *consent* to the recording. A principal party is a person in the conversation who is being spoken to or who is speaking. Consent can be express ("yes, you can record") or implied (for example, seeing the person you are having a private conversation with get out a recording device and pressing record and you not objecting). It could be argued there is no consent if, for example, a person threatens you if you do not comply with the recording.

A listening device can be legally used to record, monitor or listen to a private conversation where, for example, there is a *police warrant* allowing it.

It is legal to use a listening device to record a private conversation in certain circumstances if it is in the *public interest* such as where, for example, it is to protect the *best interests of a child*.

'Public interest' includes 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.

➢ **For example:** if a mother sets up a listening device in her child's bedroom because she suspects the child's father is sexually abusing the child, this could be argued as necessary to protect the best interests of the child and in the public interest.

It is legal to record a private conversation where a person who is a principal party in the private conversation consents to the use of the listening device (expressly or impliedly) and its use is *reasonably necessary to protect that person's lawful interest*. Only the person whose lawful interest is being protected needs to consent to the use of the listening device.

The onus of proof for establishing the above exception lies on the party seeking to establish the exception, and to prove it on the balance of probabilities (i.e. more likely than not).

Reasonably necessary for the protection of the lawful interest of that principal party:

There is a distinction between *lawful interest and legal interest*. Lawful interests are interests which are not unlawful; its meaning is similar to the expressions 'legitimate interests' or 'interests conforming to law' – see *Farris v Boase* [2013] WASC 227 and *Violi v Berrivale Orchards Ltd* (2000) 173 ALR 518, 523 [28]. E.g. where a serious verbal dispute arises and one of the parties begins to record the dispute, as they are concerned there would otherwise be different versions of the events.

➢ **For example:** a woman has been getting constant calls from a private number, she picks up and recognises the voice to be her ex-partner who threatens to harm her. The woman installs an app on her smartphone that records telephone conversations so the next time the private number calls, she records the incoming call and his direct threats to her safety. The woman was protecting her lawful interest and can use this recording for police assistance.

Where can I find this information in the Act?

See sections 3, 5, 24 and 26 of the Act.

Use of Optical Surveillance Devices

An 'optical surveillance device' means any instrument, apparatus, equipment, or other device capable of being used to record visually or observe a private activity. It does not include spectacles, contact lenses or similar.

➢ **For example:** handheld devices such as mobile phones and tablets with a camera, cameras, drones with

cameras, binoculars, 'spy cameras'.

When is it an offence to use an optical surveillance device

Generally, it is an offence to *install*, *use*, *or maintain* an optical surveillance device to *record visually* a private activity, whether or not the person is a party to the private activity.

If a person is not a party to the private activity it is also an offence for them to *install*, *use*, *or maintain* a listening device to *observe* a private activity.

It is also an offence to *cause* an optical surveillance device to be installed, used, or maintained for one of the above purposes. E.g. paying someone to install a device for you.

Remember this prohibition is only for on *private activities*. An optical surveillance device can be used where the activity is not private, for example, using binoculars to watch a soccer match being played in a public field. Private activities are where the circumstances may reasonably be taken to indicate any of the parties to the activity desire it to only be observed by themselves. It does not include activities where those involved should have reasonably expected that activity might be observed.

Maximum penalty: $5,000 or imprisonment for 12 months or both.

For example:

- If a woman is separated but living under the same roof as her ex-partner, it would be an offence for her ex-partner to install a surveillance camera in her bedroom without her consent
- A person puts a video-camera in the bathroom of their own home to film a person getting in and out of the shower, knowing the person has not consented to being filmed in such a way
- A person deliberately leaves a laptop with its web-cam on in a bedroom to live-stream themselves having sex with a woman and the woman is unaware of the live-streaming

Where can I find this information in the Act?

See sections 3 and 6 of the Act.

When can an optical surveillance device be used?

It is legal to record visually a private activity to which you are a party if all of the principal parties to that activity *consent* to the recording. A principal party is a person who takes part in the activity. Consent can be express ("yes, you can record") or implied (e.g. seeing the person you are engaging in a private activity with get out a camera and you not objecting to them taking photos). It could be argued there is no consent if, for example, a person threatens you if you do not comply with the recording.

An optical surveillance device can be legally used to record or observe a private activity where it is carried out by a *police officer* in their normal course of duty.

It is legal to use an optical surveillance device to record a private activity in certain circumstances if it is in the *public interest* such as where, for example, it is to protect the *best interests of a child*. 'Public interest' includes 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.

- **For example:** a mother sets up an optical surveillance device in her child's bedroom because she suspects the child's father is sexually assaulting the child, this could be argued as necessary to protect the best interests of the child and in the public interest.

It is legal to *record visually* a private activity where a person who is a principal party in the private activity consents to the use of the optical surveillance device (expressly or impliedly) and its use is *reasonably necessary to protect that person's lawful interest*. Only the person whose lawful interest is being protected needs to consent to the optical surveillance devices use.

The onus of proof for establishing the above exception lies on the party seeking to establish the exception, and to prove it on the balance of probabilities (i.e. more likely than not).

Reasonably necessary for the protection of the lawful interest of that principal party:

There is a distinction between *lawful interest* and *legal interest*. Lawful interests are interests which are not unlawful; its meaning is similar to the expressions 'legitimate interests' or 'interests conforming to law' – see *Farris v Boase* [2013] WASC 227 and *Violi v Berrivale Orchards Ltd* (2000) 173 ALR 518, 523 [28].

For example:

- A woman begins to visually record her ex-partner at changeover for the children because he is physically intimidating her and begins throwing objects at her
- A person sets up surveillance cameras on their property to protect themselves from theft or trespass.

Where can I find this information in the Act?

See sections 6, 24 and 27 of the Act.

Use of Tracking Devices

A 'tracking device' means any instrument, apparatus, equipment, or other device capable of being used to determine the geographical location of a person or object.

- **For example:** GPS tracking device, mobile phones with GPS tracking activated, a desktop computer/ laptop/mobile device linked to a GPS tracker on the person being tracked.

When is it an offence to use a tracking device

It is an offence to *attach*, *install*, *use*, *or maintain* a tracking device to determine the geographical location of a person without their permission, or to determine the geographical location of an object without the permission of the person in possession or having control of that object.

It is also an offence to *cause* a tracking device to be attached, installed, used, or maintained for one of the above purposes. E.g. paying someone to install a tracking device for you.

Maximum penalty: $5,000 or imprisonment for 12 months, or both.

For example:

- A person cannot give a person a smartphone that has software loaded on to it that they use to monitor the person's movements without that person's permission
- A person cannot put a GPS tracking device onto another person's car

Where can I find this information in the Act?

See section 7 of the Act.

When can a tracking device be used?

A tracking device can only be legally used with the *express or implied consent* 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.

A tracking device can also be legally used by a *police officer* in their normal course of duty.

Where can I find this information in the Act?

See section 7 of the Act.

Sharing of Private Conversations or Activities

When is it an offence to share private conversations or activities

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

Maximum penalty: $5,000 or 12 months imprisonment (or both).

For example:

- A person uses a listening device to monitor another person's private telephone conversations without their consent then publishes the details of that conversation as a public Facebook status update
- A person has made a covert recording of another person getting undressed in private and then publishes that recording online on a public website

Where can I find this information in the Act?

See section 9 of the Act.

When can private conversations or activities be shared

There are several exceptions that apply, including:

- Where the publication or communication is *made to a party* to the private conversation or the private activity. E.g. sending an electronic version of the recording to the other person who was a party to the conversation
- Where all of the other principal parties to the private conversation or activity *consent* (expressly or impliedly) to it being published or communicated
- To *protect the lawful interests* of the person and the publication or communication was not more than was reasonably necessary to protect their interest
- Where the person making the publication or communication believes on reasonable grounds that it was necessary to make that publication or communication in connection with an *imminent threat of serious violence to persons or of substantial damage to property*
- Where a *judge has made an order* that it may be communicated or published

Where can I find this information in the Act?

See sections 9 and 31 of the Act.

Possession of a surveillance device for an unlawful purpose

It is an offence to possess a surveillance device in the knowledge that it is *intended or principally designed for an unlawful use*.

Maximum penalty: $5,000 or imprisonment for 12 months or both.

Where can I find this information in the Act?

See section 34 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 instals 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 WA*** and the ***Legal Guide to Relevant Criminal Offences in WA*** for further information.

March 2022

WESNET
The Women's Services Network

WOMEN'S LEGAL SERVICE NSW

For more information on technology safety and to download resources including national legal guides, go to **www.techsafety.org.au/resources**