NEW SOUTH WALES

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN NEW SOUTH WALES

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 NSW

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 in NSW..

For information on other areas of law see:

Legal Guide to Relevant Criminal Offences in NSW

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 Apprehended Violence Orders in NSW

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In NSW these protection orders are called Apprehended Violence Orders (AVOs).

Legal Guide to Image-Based Abuse in NSW

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 dollar amount for one penalty unit is set out in section 17 of the Crimes (Sentencing and Procedure) Act 1999 (NSW). As of July 2021, one penalty unit = $110 (for individuals). Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of $5,500.

SURVEILLANCE LEGISLATION IN NEW SOUTH WALES

Surveillance Devices Act 2007 (NSW)

The *Surveillance Devices Act 2007* (NSW) (the 'Act') regulates the installation, use, maintenance and retrieval of surveillance devices in NSW.

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

A 'device' includes instruments, apparatus and equipment.

Where can I find this information in the Act?

See section 4 of the Act for definitions of terms used in 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. Common examples: Handheld devices such as mobile phones and tablets, which have inbuilt audio recording capabilities; voice recorders/dictation equipment, audio bug surveillance devices.

Note that a device is considered a listening device even if it is also capable of recording or transmitting a visual image (example: a video camera), or recording or transmitting its own position.

When is it an offence to use a listening device

Generally, it is an offence to knowingly install, use or cause to be used, or maintain a listening device to **record** a private conversation, whether or not the person is a party to that private conversation.

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

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

➢ **For example:** It is an offence for a person to install an audio bug surveillance device in his home in order to overhear, 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/record both sides of the telephone conversation then it would also be a federal offence under the *Telecommunications (Interception and Access) Act 1979* (Cth).

When can a listening device be used

It is legal to record a conversation to which the person is a party to if all parties consent, expressly or impliedly, to the listening device being used.

It is also legal to record a conversation to which a person is a party to if one principal party (e.g. the person recording) consents to the recording of the conversation and it is either:

- reasonably necessary for the protection of the lawful interest of that principal party (see note below), or
- the recording is not made for the purpose of communicating or publishing the conversation or a report of it to persons who are not parties to the conversation.

The onus of proof for establishing the above exception lies on the party seeking to establish the exception, and that onus is on the balance of probabilities.

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 *Violi v Berrivale Orchards Ltd* (2000) 173 ALR 518, 523 [28].

Whether a recording is reasonably necessary for the protection of the lawful interests of a party is objectively determined, having regard to the lawful interest existing at the time of making the recording. See *Corby & Corby* [2015] FCCA 1099 (16 April 2015) [19] for discussion of what constitutes a 'lawful interest'.

For example:

- ➢ A person in need of protection covertly records the abuse/assaults directed at her.
  It is not an offence for a woman being assaulted by her partner to record the assault secretly (e.g. mobile phone set to record and placed in her pocket).
- ➢ A person in need of protection records child contact changeovers.

It is not an offence for one party to record a changeover at McDonalds with the other party because it is in a public space, with no reasonable expectation that conversation will not be heard by others.

Where can I find this information in the Act?

See sections 4 and 7 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. Common examples: handheld devices such as mobile phones and tablets with a camera, cameras, binoculars, 'spy cameras'.

When is it an offence to use an optical surveillance device

Generally, if the installation, use or maintenance of an optical surveillance device involves:

- entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle; or
- interference with the vehicle or other object without the express or implied consent of the person having lawful possession or lawful control of the vehicle or object,

it will be an offence to knowingly install, use or maintain an optical surveillance device on or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity.

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

For example:

- ➢ It is an offence for a person to break into his ex-partner's house or enter her property without her consent to install a surveillance camera.
- ➢ It is an offence for a person to break into his ex-partner's vehicle to install a surveillance camera.

When can an optical surveillance device be used

As long as the installation, use or maintenance of an optical surveillance device does not involve the unauthorised entry onto/into a premise or vehicle or unauthorised interference with a vehicle or other object, it is not an offence under section 8 of this Act.

- ➢ **For example:** A person may generally install surveillance cameras on their property.

However, the use of the surveillance cameras might be in contravention of other laws. For example, it would be a criminal offence for a person to install a surveillance camera in the bathroom of his own home to film a person getting in and out of the shower, knowing that the person has not consented to being filmed in such a way. For relevant criminal offences, please see the ***Legal Guide to Relevant Criminal Offences in NSW*** and the ***Legal Guide to Image-Based Abuse in NSW.***

Where can I find this information in the Act?

See sections 4 and 8 of the Act.

Use of Tracking Devices

A 'tracking device' means any electronic device capable of being used to determine or monitor the geographical location of a person or an object. Common examples: 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

Generally, it is an offence to knowingly 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 lawful possession or having lawful control of that object.

It is an offence to track someone's geographical location without their consent by using:

- a standalone GPS tracking device
- an application on a person's mobile phone that tracks GPS location
- any other application or program such as 'find my iPhone'

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

➢ **For example:** It is an offence for a person to install a tracking device in their ex-partner's car to monitor her location.

When can a tracking device be used

The only exceptions that apply relate to using a tracking device 'for a lawful purpose'. There is no case law or commentary about what the court considers a 'lawful purpose' to be. In the absence of any direct guidance, the meaning of a 'lawful purpose' could be taken to be similar to the meaning of a 'lawful interests' (as used in relation to an exception where a listening device may be used). See *Corby & Corby* [2015] FCCA 1099 (16 April 2015) [19] for discussion of what constitutes a 'lawful interest'.

Where can I find this information in the Act?

See sections 4 and 9 of the Act.

Use of Data Surveillance Devices

A 'data surveillance device' means any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device. Common examples: Computer and mobile phone spyware such as mSpy and SniperSpy.

Note: Smartphones are considered computers under this legislation.

When is it an offence to use a data surveillance device

Generally, a person must not knowingly install, use or maintain a data surveillance device on or in premises to record or monitor the input of information into, or the output of information from, a computer on the premises if the installation, use or maintenance of the device involves:

- entry onto or into the premises without the express or implied consent of the owner or occupier of the premises, or
- interference with the computer or a computer network on the premises without the express or implied consent of the person having lawful possession or lawful control of the computer or computer network.

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

For example:

➢ A person cannot enter premises (home/office) without the permission of the owner or occupier of those premises to install a data surveillance device on a computer within.

➢ A person, even if permitted to be on/in premises, cannot interfere with a computer to install a data surveillance device without the permission of the person having lawful possession or lawful control of the computer.

➢ A person cannot install a data surveillance device on a computer remotely (such as by using malware as a carrier) as it would involve interference with the computer or its network without the permission of the person having lawful possession or lawful control of the computer.

Where can I find this information in the Act?

See sections 4 and 10 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

If a person has knowledge of a private conversation or the carrying on of an activity that was obtained directly or indirectly through the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of Part 2 of the Act (Regulation of installation, use and maintenance of surveillance devices), that person is prohibited from publishing or communicating to any person:

- knowledge of the private conversation; or
- a record of the carrying on of the activity, or
- a report of a private conversation or carrying on of an activity.

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

'*Record*' includes the following:

(a) an audio, visual, or audio-visual record

(b) a record in digital form

(c) a documentary record prepared from a record referred to in (a) or (b)

'*Report of*' a conversation or activity includes a report of the substance, meaning or purport of the conversation or activity.

Where can I find this information in the Act?

See sections 4 and 11 of the Act.

When can a private conversation or recordings of activities be shared

There are several exceptions that apply. Most relevantly in this context, communication or publication is allowed if it is no more than is reasonably necessary in connection with an imminent threat of serious violence to persons or of substantial damage to property.

Knowledge of a private conversation or recordings of activities can be shared if it was also obtained in a manner that did not contravene Part 2.

Where can I find this information in the Act?

See sections 4 and 11 of the Act.

Possession of a Record of a Private Conversation or Activity

When is it an offence to possess a record of a private conversation or activity

Generally, it is an offence for a person to possess a record of a private conversation or the carrying on of an activity if they know that it has been obtained, directly or indirectly, by the use of a listening device, optical surveillance device, or tracking device in contravention of Part 2.

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

When can a person legally possess a record of a private conversation or activity

One exception is if the principal parties to the private conversation or the persons who took part in the activity consent to the person possessing a record of the private conversation or activity.

Another exception is if the person possesses the record as a consequence of the record being shared with that person in a manner that does not contravene Part 2.

Where can I find this information in the Act?

See section 12 of the Act.

Sharing of Information from the Use of a Data Surveillance Device

When is it an offence to share information obtained from the use of a data surveillance device

A person must not publish, or communicate to any person, any information regarding the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a data surveillance device in contravention of this Part.

Note: This is similar to section 11 of the Act in relation to the sharing of private conversations of recordings of activities.

Maximum penalty: 100 penalty units or imprisonment for 5 years, or both.

- **For example:** It is an offence for a person to access his ex-partner's smart phone and share photographs of her that he finds there online. This behaviour may also constitute an offence under the *Crimes Act 1900* (NSW). See the ***Legal Guide to Image-Based Abuse in NSW*** and the ***Legal Guide to Relevant Criminal Offences in NSW*** for more information.

When can information obtained from the use of a data surveillance device be shared

There are several exceptions that apply. Most relevantly in this context, communication or publication is allowed if it is no more than is reasonably necessary in connection with an imminent threat of serious violence to persons or of substantial damage to property.

Where can I find this information in the Act?

See section 14 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 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 NSW*** and the ***Legal Guide to Relevant Criminal Offences in NSW*** 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**