NORTHERN TERRITORY

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO SURVEILLANCE LEGISLATION IN THE NORTHERN TERRITORY

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 the NT

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 the NT

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 Orders in the NT

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In the Northern Territory these protection orders are called **Domestic Violence Orders (DVOs)**.

Legal Guide to Image-Based Abuse Legislation in the NT

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 threatening violence), are known as summary offences. Summary offences are dealt with by the Court of Summary Jurisdiction.

Indictable offence

More serious offences (such as murder, manslaughter, sexual assault) are known as indictable offences and are usually dealt with by 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.

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 the Attorney-General and Justice sets the amount for one penalty unit for each year in accordance with the Penalty Units Act. As of 1 July 2021, one penalty unit = $157. Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of $7,850.

SURVEILLANCE LEGISLATION IN NORTHERN TERRITORY

Surveillance Devices Act 2007 (NT)

The *Surveillance Devices Act 2007* (NT) (the "Act") regulates the use of surveillance devices in the Northern Territory. It also restricts the use, communication and publication of information obtained through the use of surveillance devices.

A 'surveillance device' includes a data surveillance device, listening device, optical surveillance device or tracking device or a device that combines any of these purposes.

A 'device' includes an apparatus, equipment, instrument and machine.

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 a device capable of being used to listen to, monitor or record a conversation or words spoken to or by a person in a conversation. This does not include a hearing aid or similar device.

- **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 *install*, *use or maintain* a listening device knowing they do not have the consent (express or implied) of each party to the conversation, to *listen to*, *monitor or record a private conversation* to which that person is *not a party*.

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 might 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.

Remember this prohibition is only for conversations to which a person is *not a party*. A person is a 'party' to a private conversation if words are spoken by them or to them in the course of the conversation. If they are a party to the conversation, there is no prohibition on them using a listening device.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

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).

➢ 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 instals 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 has not committed an offence as she was a party to the private conversation she recorded.

Where can I find this information in the Act?

See section 11 of the Act.

When can a listening device be used

There are a number of exceptions to this offence. They include:

- Where there is a police warrant allowing it
- Where a law enforcement officer is acting in the performance of their duty and monitors or records the private conversation with the express or implied consent of at least one party to the conversation and the officer reasonably believes it is necessary to do so for the protection of someone's safety

A listening device can also be used in the *case of emergency*. For this emergency exception to apply, the person seeking to rely on the exception must show at the time of use there were reasonable grounds for believing the circumstances were so serious and the matter was of such urgency that the use of the device was is in the *public interest*.

'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, in the public interest.

If a person seeks to rely on this emergency use, they must, within two business days of starting use, provide a written report to a Judge of the Northern Territory Supreme Court. If they do not provide this report, they are guilty of an offence with a maximum penalty of 100 penalty units or imprisonment for 1 year.

The report must include:

- Particulars of the device used;
- Particulars of the use of the device and the period during which it was used;
- The name, if known, of any person whose private conversation was listened to, monitored or recorded or whose private activity was observed or visually recorded;
- The circumstances that caused the person to believe it was necessary to listen to, monitor or record the private conversation or observe or visually record the private activity; and
- The general use made or to be made of any evidence or information obtained by use of the device.

Where can I find this information in the Act?

See sections 11, 41, 43 and 45 of the Act.

Use of Optical Surveillance Devices

An 'optical surveillance device' means a device capable of being used to monitor, record visually or observe an 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

It is an offence for a person, knowing that they do not have the express or implied consent of each party to a private activity, to *install*, *use or maintain* an optical surveillance device to *monitor*, *record visually* or *observe a private activity* to which the person is *not a party*.

Remember this prohibition is only for *private* activities. An optical surveillance device can be used where the activity is not private. A "private activity" means an activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else.

Remember this prohibition is only for activities to which a person is *not a party*. A person is a 'party' to a private activity if they take part in the activity. If they are a party to the activity, there is no prohibition on them using an optical surveillance device.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

Where can I find this information in the Act?

See sections 4 and 12 of the Act.

When can an optical surveillance device be used

There are a number of exceptions to this offence. They include:

- Where there is a police warrant allowing it
- Where a law enforcement officer is acting the performance of their duty and installs, uses or maintains a device with authorisation of the occupier and it is reasonably necessary for the protection of someone's lawful interest
- Where a law enforcement officer is acting the performance of their duty and uses an optical surveillance device and it does not involve entry on a place or interference with a vehicle or other thing without permission.

An optical surveillance device can also be used in the *case of emergency*. For this exception to apply, the person seeking to rely on the exception must show at the time of use there were reasonable grounds for believing the circumstances were so serious and the matter was of such urgency that the use of the device was is in the *public interest*.

'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

If a person seeks to rely on this emergency use, they must provide the same written report as outlined above under "Use of Listening Devices".

Where can I find this information in the Act?

See sections 12, 41, 44 and 45 of the Act.

Use of Tracking Devices

A 'tracking device' means an electronic device that may be used to determine the geographical location of a person or thing.

➢ **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 for a person to *install*, *use or maintain* a tracking device to determine the *geographic location of another person*, knowing that they have done so without the express or implied consent of that person.

It is also an offence for a person to *install*, *use or maintain* a tracking device to determine the *geographic location of a thing*, knowing that they have done so without the express or implied consent of the person in lawful possession or who has lawful control of that thing.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

When can a tracking device be used

The exceptions to this offence are limited and include:

- Where there is a police warrant allowing it

- Where a law enforcement officer is acting the performance of their duty and instals the device on a thing in a public place. E.g. the police officer investigating a matter attaches a tracking device to a suspect's car on a street.

Where can I find this information in the Act?

See sections 4 and 13 of the Act.

Use of Data Surveillance Devices

A 'data surveillance device' means a device capable of being used to monitor or record the information being put on to or retrieved from a computer, but does not include an optical surveillance device.

The legislation 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 *Criminal Code 1983* (NT) sections 276B to 276D 'computer offences'. For further information please see the ***Legal Guide to Relevant Criminal Offences in the NT***.

Where can I find this information in the Act?

See section 14 of the Act.

Sharing of Private Conversations and Activities

When is it an offence to share private conversations or activities

It is an offence for a person to *communicate or publish* a record or report of a private conversation or private activity, knowing that the record or report 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: 250 penalty units or imprisonment for 2 years.

Common scenarios:

- ➢ A person uses a listening device to monitor another person's private telephone conversations without their consent then publishes the details of a conversation they were not involved in as a public Facebook status update
- ➢ A person has made a covert recording of another person getting undressed in private publishes that recording online on a public website

Where can I find this information in the Act?

See section 15 of the Act.

When can a private conversation or recordings of activities be shared

There are a number of exceptions to this offence. They include:

- Where each party to the private conversation or private activity impliedly or expressly consented to the communication or publication
- Where the communication or publication was no more than was reasonably necessary for the *protection of the lawful interests* of the person making it
  - E.g. a woman could report to police if she used a listening device to record a private conversation between her ex-partner and an accomplice discussing their intentions to harm her.
- Where the information is being communicated or published in the course of legal or disciplinary proceedings
- Where the communication or publication was made by a law enforcement officer while performing their duties

If a person has used a listening device or an optical surveillance device in accordance with the *emergency use in public interest* exceptions (sections 43 and 44), they can apply for a court order to allow them to publish or communicate a private conversation, a report or record of a private conversation, or a record of a private activity.

A judge can only make such an order if satisfied the publication or communication should be made to protect or further the public interest.

Where can I find this information in the Act?

See sections 15 and 46 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 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 a 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 conduct in relation to technology-facilitated stalking or abuse may constitute a criminal offence. Please see the ***Legal Guide to Image-based Abuse in the NT*** and the ***Legal Guide to Relevant Criminal Offences in the NT*** 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**