WESTERN AUSTRALIA

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES 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 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.

For information on other areas of law see:

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.

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 (including in non-heterosexual relationships), 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.

RELEVANT CRIMINAL OFFENCES

Some forms of technology-facilitated stalking and abuse are against the law. If it is unlawful, then the person responsible can be charged with a criminal offence.

This guide will look at some of the offences under **Western Australian** and **Commonwealth** laws that are relevant to technology-facilitated stalking and abuse.

Note: The *Surveillance Devices Act 1998* (WA) and the *Restraining Orders Act 1997* (WA) also contain relevant offences – these offences are covered in the ***Legal Guide to Surveillance Legislation in WA*** and the ***Legal Guide to Family Violence Restraining Orders in WA***. Intimate image offences are covered in the **Legal Guide to Image-Based Abuse in WA**.

This guide covers the following legislation:

Criminal Code Act 1913 (WA)

1. Threat with intent to gain etc. (s 338A)
2. Threats (s 338B)
3. Statement or act creating false apprehension as to existence of threat or danger (s 338C)
4. Stalking (s 338E)
5. Criminal defamation (s 345)
6. Threats or demands to extort (s 397 & s 398)
7. Unlawful use of computer (s 440A)
8. Making, using or supplying identification material with intent to commit indictable offence (s 490)

Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA)

9. Leaving publications in certain places (s 65E)
10. Unclassified, RC and X 18+ films, sale of (s 73)
11. Leaving films in certain places (s 80)
12. Possession or copying of certain films (s 81)

Criminal Code 1995 (Cth)

13. Dealing in identification information (s 372.1)
14. Interception devices (s 474.4)
15. Offences using a carriage service
    - To make a threat (s 474.15)
    - To menace, harass or cause offence (s 474.17)

Telecommunications (Interception and Access) Act 1979 (Cth)

16. Telecommunication not to be intercepted (s 7)
17. No dealing in intercepted information or interception warrant information (s 63)
18. Civil remedies unlawful interception or communication (s 107A)

Criminal Code Act 1913 (WA)

1. Threats (sections 338A-338C)

Threats include those to kill, injure or endanger a person, or to destroy, endanger or harm property or to take control of a building by force or violence or to cause a detriment of any kind to a person (see s 338).

Threats with intent to gain (section 338A)

It is an offence for a person to make a threat with intent to:

- Gain a benefit (does not have to be monetary); or
- Cause a detriment (does not have to be monetary); or
- Prevent or hinder someone doing an act they are lawfully entitled to do; or
- Compel someone to do an act where they are lawfully entitled to not do that act

Maximum penalty: imprisonment for seven years, unless the offence involved a threat to kill, in which case imprisonment for 10 years.

➢ **For example:** a person threatens his ex-partner that he will upload a sex tape of her online if she does not pay him money.

2. Threats (section 338B)

It is an offence to threaten to:

- Kill, injure or endanger a person; or
- To destroy, endanger or harm property; or
- To take control of a building by force or violence; or
- To cause a detriment of any kind to a person

Maximum penalty: imprisonment for 3 to 14 years, depending on the circumstances.

➢ **For example:** in a 2015 unreported case, a man was found guilty of this offence where he sent text messages to a woman he had been in a brief relationship with, asking her to upload a sex tape they had made onto a porn sharing website. When she refused, he sent messages to the victim demanding nude photos. He was fined $2,000 with no criminal conviction recorded.

3. Statement or act creating false apprehension as to existence of threat or danger (section 338C)

It is an offence to make a statement or to convey information knowing it is false, which indicates that a threat has been made or there is an intention, proposal or plan to:

- Kill, injure or endanger a person; or
- To destroy, endanger or harm property; or
- To take control of a building by force or violence; or
- To cause a detriment of any kind to a person

Maximum penalty: imprisonment for 3 to 14 years, depending on the circumstances.

➢ **For example:** a person makes up a lie, telling his ex-partner that his brother was using his computer when he found naked photos of her, and his brother now plans to post them online

4. Stalking (section 338E)

Intimidate includes:

- Causing physical or mental harm; or
- Causing apprehension or fear; or
- Preventing or hindering someone doing an act they are lawfully entitled to do; or
- Compelling someone to do an act where they are lawfully entitled to not do that act.

Pursue includes:

- Repeated intentional communication; or
- Repeatedly intentional following someone; or
- Watching or approaching a place where a person lives, works or happens to be; or
- Breaching a restraining order or bail condition.

Stalking with intent to intimidate (section 338E(1))

It is an offence for a person to pursue another with the intent to intimidate them or a third person.

Maximum penalty: imprisonment for 3 years or 8 years if aggravated.

➢ **For example:** a person repeatedly text messages and calls his ex-partner stating that he is watching her and is going to "get her" and it can be shown he intended to intimidate her.

Stalking generally (section 338E(2))

It is an offence for a person to pursue another in a manner that could reasonably be expected to, and in fact does, intimidate the other person.

Maximum penalty: imprisonment for 12 months and a fine of $12 000.

➢ **For example:** a person repeatedly calls his ex-partner and hangs up before she can pick up the phone. This happens about 10 times a day over a week. He argues that he just wanted to talk but would get nervous and hang up. The victim feels intimidated, and this behaviour could reasonably be expected to intimidate the victim, even if it was not his intention.

5. Criminal defamation (section 345)

It is an offence for a person to publish defamatory material about another living person without a lawful excuse and:

- Knowing the matter to be false or without having regard to whether it is true or false; and
- Intending to cause serious harm or without having regard to whether it will cause harm.

A person has lawful excuse if they can prove they would have a defence to civil law defamation. Some defences include proving the defamatory allegations are substantially true or are a fair report of proceedings (e.g. a court matter) or that it was an honest opinion with a proper basis or that the matter is trivial and it is unlikely the defamed person suffered any harm.

Maximum penalty: Imprisonment for 3 years.

➢ **For example:** a person posts on the Facebook page of a school where his ex-partner works as a teacher. He makes up false accusations that his ex-partner is having sex with students at the school, and as a consequence, her reputation is damaged.

6. Threats or demands to extort etc. (sections 397 & 398)

It is an offence to:

- Make written or oral threats of injury or detriment of any kind (s 397); or
- Accuse or threaten to accuse a person of committing an indictable offence (s 398)

to extort or gain anything from that person.

Maximum penalty: imprisonment for 14 - 20 years, depending on the circumstances.

➢ **For example:** a person tells his ex-partner he will make up a lie and tell the police she is sexually abusing their child unless she agrees to film a sex tape with him.

7. Unlawful use of computer (section 440A)

It is an offence for a person to use a *restricted-access computer* where they are not authorised to do so or where they do not use it in accordance with their authorisation. The person will be liable if they intend to or do in fact gain a benefit or cause detriment to the owner (does not have to be monetary).

Use means to gain access to information stored in the system or operate the system in some other way.

Restricted-access computer is one that requires a password, which is only known to the user.

Maximum penalty: imprisonment for 2 to 10 years, depending on the circumstances.

➢ **For example:** a person hacks into his ex-partner's computer and deletes all of her files.

8. Making, using or supplying identification material with intent to commit indictable offence (section 490)

It is an offence for a person to make, use or supply identification material with the intention that the material will be used to commit an indictable offence.

Identification information could include, for example a person's name, address, date or place of birth, marital status, relatives, bank details or records of their details.

Maximum penalty: imprisonment for seven years or the maximum penalty for the indictable offence the convicted person intended to commit, whichever is greater.

➢ **For example:** a man posts his ex-partner's name, photo and address on a forum instructing other people on the forum to go to her house and rape her.

➢ When someone posts a person's personal identification information online in this manner, it is sometimes referred to as 'doxing'.

Classification (Publications, Films and Computer Games) Enforcement Act 1996 (WA)

Refused classification (RC) includes, for example, films that deal with sex, crime, cruelty or violence in way that offends the standards of morality, decency and propriety generally accepted by reasonable adults (*National Classification Code (May 2005)*).

X 18+ includes, for example, films (that are not RC) that contain real depictions of actual sexual activity between consenting adults that would be unsuitable for a minor to see (*National Classification Code (May 2005)*).

R 18+ includes, films (that are not RC or X 18+) that are unsuitable for a minor to see (*National Classification Code (May 2005)*).

MA 15+ includes, films (that are not RC, X 18+ or R 18+) that deal with sex, violence or coarse language in such a manner as to be unsuitable for viewing by persons under 15 (*National Classification Code (May 2005)*).

9. Leaving publications in certain places (section 65E)

It is an offence for a person to leave a publication (can be written or pictorial) in a public place, or so it is visible in a public place, where:

- If it if ever put before a classification board, it would be likely to be classified *Refused Classification*; or
- Where it would cause offence to a reasonable adult; or
- Where it would be unsuitable for a minor to see.

Maximum penalty: $10 000.

➢ **For example:** a person prints out naked photos of his ex-partner and pastes them on street poles around her neighbourhood.

10. Unclassified, RC and X 18+ films, sale of (section 73)

It is an offence for a person to sell an unclassified film.

Maximum penalty: $15 000 or imprisonment for 18 months.

➢ **For example:** a person sells online a tape he made of himself and his ex-partner having sex.

11. Leaving films in certain places (section 80)

It is an offence for a person to leave a film in a public place or on private premises (without the occupier's permission), where it if ever put before a classification board, that film would be classified *X 18+*.

Maximum penalty: $5,000

➢ **For example:** a person leaves a sex tape of his ex-partner on her parent's doorstep.

12. Possession or copying of certain films (section 81)

Possession or copying refused classification film (section 81(1))

It is an offence for a person to possess or copy a film where it would be *refused classification* if ever put before a classification board.

Maximum penalty: $10,000

Possession or copying X 18+, R 18+ or MA 15+ film (section 81(2))

It is an offence for a person to possess or copy a film with the intention of exhibiting it or selling it, where that film would be classified *X 18+*, *R 18+* or *MA 15+* if it were ever put before a classification board.

If the person was in possession of, or made 10 or more copies of the film, that is sufficient to prove the person had the intention of exhibiting or selling the film, in the absence of contrary evidence.

Maximum penalty: $10,000

Criminal Code 1995 (Cth)

13. Dealing in identification information (section 372.1)

It is an offence to **make**, **supply** or **use** the identification information of another person to pretend to be, or to pass oneself off as another person for the purpose of committing or facilitating a Commonwealth indictable offence (meaning, a crime under a Commonwealth Act that is punishable by imprisonment for more than 12 months).

This is commonly referred to as 'identity fraud'.

Maximum penalty: Imprisonment for 5 years.

➢ **For example:** a person makes a social media account in his ex-partner's name, pretending to be her. He posts her personal details and tries to add her friends so they see the account. In order to harass her, he starts posting offensive comments from this account (see also s 474.17).

14. Interceptions devices (section 474.4)

It is an offence to *manufacture*, *advertise*, *sell*, or *possess* an interception device.

Interception device includes an apparatus or device that is capable of intercepting a communication passing over a telecommunication system that could reasonably be regarded as having been designed for that purpose (see s 473.1).

Maximum penalty: Imprisonment for 5 years.

➢ **For example:**it is an offence for a person to have in their possession an audio bugging device used to intercept and listen to phone calls.

15. Offences relating to the use of a carriage service (sections 474.15 and 474.17)

A 'carriage service' means a service for carrying communications by means of guided and/or unguided electromagnetic energy (s 7 *Telecommunications Act 1997* (Cth)). Examples include:

- Telephone services
- Internet access services
- Voice over Internet Protocol (VoIP) services (eg, Skype)

Using a carriage service to make a threat to kill (s 474.15)

It is an offence for a person to use a carriage service to make a *threat* to a person that they will **kill** them or a third person, intending them to fear the threat will be carried out. It is not necessary to prove that the person receiving the threat actually feared that the threat would be carried out.

Maximum penalty: Imprisonment for 10 years.

- ➢ **For example:** sending a person a text message, email or instant message or a telephone or videoconference call where they threaten to kill their ex-partner or her child

Using a carriage service to make a threat to cause serious harm (s 474.15)

It is also an offence for a person to use a carriage service to make a threat to a person that they will cause them or a third person *serious harm*, intending them to fear the threat will be carried out. It is not necessary to prove that the person receiving the threat actually feared that the threat would be carried out.

Maximum penalty: Imprisonment for 7 years.

- ➢ **For example:** sending a person a text message, email or instant message or a telephone or videoconference call where they threaten to break the limbs of their ex-partner or her child

Using a carriage service to menace, harass or cause offence (s 474.17)

It is an offence for a person to use a carriage service in a way that reasonable persons would regard as being menacing, harassing or offensive.

Maximum penalty: Imprisonment for 3 years.

- ➢ **For example:** sending a person a large volume of offensive text messages, emails or instant messages or a telephone or videoconference calls

Telecommunications (Interception and Access) Act 1979 (Cth)

16. Interception of telecommunications (section 7)

It is an offence for a person to intercept or do any act or thing that will enable that person or another person to *intercept a communication passing over a telecommunications system*.

Interception of a communication passing over a telecommunications system means listening or recording the communication without the knowledge of the person making the communication.

There are limited exceptions, for example, where there was a warrant issued.

Maximum penalty: Imprisonment for 2 years (see s 105).

- ➢ **For example:** someone pays a person to set up a phone bug on their ex-partners phone without their knowledge, to listen in on their calls.
- ➢ Due to the definition of *passing over* (s 5F) it would not be an offence to read a person's inbox of emails or SMS messages without their consent because the messages have already been received and are not in transit

17. Dealing in intercepted information (section 63)

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).

- 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

18. Civil remedies relating to unlawful interception and communication (section 107A)

The legislation provides for civil remedies for the unlawful interception of a communication passing over a telecommunications system, and the unlawful communication of such information.

Some orders the court can make are:

- An order declaring the interception or communication was unlawful
- An order that the defendant pay to the protected person damages or another amount representing the income derived by the defendant from the interception
- An injunction

Online Safety Act 2021 (Cth)

The *Online Safety Act 2021* (Cth) is legislation that attempts to keep Australians safe online and includes mechanisms to have abusive and harmful content removed from online. It is civil legislation not criminal, however may be relevant if there are criminal charges being laid in relation to distributing intimate images without consent. In addition to pressing criminal charges the images can be reported to the eSafety Commissioner in an attempt to have the images removed.

The Office of the eSafety Commissioner (OeSC) can investigate complaints of abusive and harmful material online and issue removal notices to service or hosting providers and/or the user (abuser). Complaints can be made at esafety.gov.au.

- **Non-consensual sharing of images** (Part 6) - see the ***Legal Guide to Image-Based Abuse Legislation*** handout for each State for more information about the *Online Safety Act 2021* (Cth).

- **Cyber-abuse material targeting an Australian adult** (Part 7). Establishing cyber-abuse requires that:
  - an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult (physical harm and/or harm to mental health); and
  - an ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive.

  Maximum penalty for non-compliance with removal notice**:** 500 penalty units.

- **Cyber-bullying material targeting an Australian child** (Part 5). Establishing cyber-bullying requires that:
  - an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect on a particular Australian child; and
  - the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child.

  Maximum penalty for non-compliance with removal notice**:** 500 penalty units.

You can find more information about the Online Safety Act 2021 at https://www.esafety.gov.au/

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

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**