VICTORIA

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES IN VICTORIA

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 VIC

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 VIC

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 Intervention Orders in VIC

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In Victoria these protection orders are called **Family Violence Intervention Order (FVIOs)**.

Legal Guide to Image-Based Abuse Legislation in VIC

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.

DISCLAIMER: The use of technology-facilitated abuse is a developing area of the law. The legal information, examples and scenarios contained in the guide are intended to explain the law as it stands at publication in general terms only and are not legal advice. They cannot be relied upon or applied by readers in their own cases. Each set of circumstances needs to be looked at individually. You should seek legal advice about your own particular circumstances.

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 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 Department of Treasury and Finance set the dollar amount for one penalty unit; this value is updated on 1 July each year. As of 1 July 2021: one penalty unit = $181.74.

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 looks at some of the offences under Victorian and Commonwealth law that are relevant to technology-facilitated stalking and abuse.

Note: *The Surveillance Devices Act 1999* (Vic) and *Family Violence Protection Act 2008* (Vic) also contain relevant offences – these offences are covered in the ***Legal Guide to Surveillance Legislation in VIC*** and the ***Legal Guide to Family Violence Intervention Orders in VIC***. The offences contained in the *Summary Offences Act 1966* (Vic) are covered in greater detail in the ***Legal Guide to Image-Based Abuse in VIC***.

This guide covers the following legislation:

Crimes Act 1958 (Vic)

1. Threats to kill (s 20)
2. Threats to inflict serious injury (s 21)
3. Stalking (s 21A)
4. Conduct endangering persons (s 23)
5. Extortion with threat to kill (s 27)
6. Extortion with threat to destroy property etc. (s 28)
7. Threat to assault (s 31(1))
8. Blackmail (s 87)
9. Making, using or supplying identification information (s 192B)
10. Threats to destroy or damage property (s 198)
11. Unauthorised modification of data to cause impairment (s 247C)
12. Unauthorised impairment of electronic communication (s 247D)
13. Unauthorised access to or modification of restricted data (s 247G)

Summary Offences Act 1966 (Vic)

14. Observation of genital or anal region (s 41A)
15. Visually capturing genital or anal region (s 41B)
16. Distribution of an image of genital or anal region (s 41C)
17. Distribution of intimate image (s 41DA)
18. Threat to distribute intimate image (s 41DB)

Criminal Code 1995 (Cth)

19. Dealing in identification information (s 372.1)
20. Interception devices (s 474.4)
21. 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)

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

Crimes Act 1958 (Vic)

1. Threats to kill (section 20)

It is an offence to make a threat to kill to another person intending them to fear the threat would be carried out or being reckless to their fear.

Maximum penalty: Imprisonment for 10 years.

➢ **For example:** a person sends his ex-partner a text message saying that he will kill her or her child and because of the history of domestic violence she feared it would be carried out.

2. Threats to inflict serious injury (section 21)

It is an offence to make a threat to inflict serious injury on another person intending them to fear the threat would be carried out or being reckless to their fear.

Maximum penalty: Imprisonment for 5 years.

➢ **For example:** a person sends his ex-partner a private message on social media stating in detail how he will break her legs

3. Stalking (section 21A)

It is an offence to stalk another person.

Stalking is where the offender engages in a *course of conduct*, with the intention of causing physical or mental harm to the victim, including self-harm, or of arousing apprehension or fear in the victim for their safety or that of any other person.

An offender has the requisite intention if they knew the kind of course of conduct would be likely to cause harm or arouse apprehension or fear or they ought to have understood that likelihood in the circumstances and it caused actual harm, apprehension or fear.

A *course of conduct* includes any of the following:

- Following the victim or any other person
- Contacting the victim or any other person by post, telephone, fax, text message, e-mail or other electronic communication or any other means
- Publishing on the Internet or by an e-mail or other electronic communication a statement or other material relating to the victim or any other person; or purporting to relate to, or to originate from, the victim or any other person
- Causing an unauthorised computer function in a computer owned or used by the victim or any other person
- Tracing the victim's or any other person's use of the Internet or of e-mail or other electronic communications
- Entering or loitering outside or near the victim's or any other person's place of residence or of business or any other place frequented by the victim or the other person
- Interfering with property in the victim's or any other person's possession (whether or not the offender has an interest in the property)
- Making threats to the victim
- Using abusive or offensive words to or in the presence of the victim
- Performing abusive or offensive acts in the presence of the victim
- Directing abusive or offensive acts towards the victim
- Giving offensive material to the victim or any other person or leaving it where it will be found by, given to or brought to the attention of, the victim or the other person
- Keeping the victim or any other person under **surveillance**
- Acting in any other way that could reasonably be expected to cause physical or mental harm to the victim or to arouse apprehension or fear for safety

Maximum penalty: Imprisonment for 10 years.

4. Conduct endangering persons (section 23)

It is an offence to recklessly engage in conduct that places or may place another person in danger of serious injury is guilty of an indictable offence.

Maximum penalty: Imprisonment for 5 years.

- **For example:** a man publishes on the internet an advertisement with his ex-girlfriend's picture, name, and address and states on the advertisement that she enjoys rough sex and 'rape' scenarios.

5. Extortion with threat to kill (section 27)

It is an offence to make a demand of another person with a threat to kill or inflict injury on a person or with a threat that would endanger the life of a person if it were carried out.

Maximum penalty: Imprisonment for 15 years.

- **For example:**a person tells their ex-partner over social media that if she does not hand over the children, he will come and shoot her

6. Extortion with threat to destroy property etc. (section 28)

It is an offence to make a demand of another person with a threat to destroy, or endanger the safety of a building or structure.

Maximum penalty: Imprisonment for 10 years.

- **For example:** a person tells their ex-partner over social media that if she does not hand over the children, he will burn down her house.

7. Threat to assault (section 31(1))

It is an offence to threaten to assault another person with intent to commit an indictable offence.

Maximum penalty: Imprisonment for 5 years.

- **For example:** a person calls their ex-partner and tells her he is coming to 'bash her'.

8. Blackmail (section 87)

It is an offence to blackmail a person with a view to gain or with intent to cause loss to another, by making an unwarranted demand with menace.

Maximum penalty: Imprisonment for 15 years.

- **For example:** a person demands money from his ex-partner and tells her if she does not comply, he will post a sex tape of her on the internet.

9. Making, using or supplying identification information (section 192B)

It is an offence to make, use or supply identification information intending to use or supply the information to commit or facilitate the commission of an indictable offence.

Maximum penalty: Imprisonment for 5 years.

- **For example:**a man publishes on the internet an advertisement with his ex-girlfriend's picture, name, and address and tells people to go to her house and rape her.

10. Threats to destroy or damage property (section 198)

It is an offence to make a threat to destroy or damage any property belonging to another person or one's own property in a way that is likely to endanger the life of a person, made with the purpose of causing the other to fear it would be carried out.

Maximum penalty: Imprisonment for 5 years.

- **For example:**a person sends his ex-partner a text message saying that he will blow up her car.

11. Unauthorised modification of data to cause impairment (section 247C)

It is an offence to cause unauthorised modification of data held in a computer, knowing it is unauthorised and with the intention of impairing access to, or impairing reliability, security or operation of any data in a computer or recklessness to such impairment

Maximum penalty: Imprisonment for 10 years.

- ➢ **For example:** a man infects his ex-partner's computer with a virus so she can no longer access her computer files.

12. Unauthorised impairment of electronic communication (section 247D)

It is an offence to intentionally cause unauthorised impairment of electronic communication to or from a computer knowing the impairment is unauthorised or being reckless to such impairment.

Maximum penalty: Imprisonment for 10 years.

- ➢ **For example:** a man infects his ex-partner's computer with a virus so she can no longer send emails from her computer.

13. Unauthorised access to or modification of restricted data (section 247G)

It is a summary offence to intentionally cause any unauthorised access to or modification of restricted data held in a computer, knowing the access or modification is unauthorised.

Restricted data includes data restricted by an access control system, for example, where you need a password to log in to the computer.

Maximum penalty: Imprisonment for 2 years.

- ➢ **For example:** a person hacks in to his ex-partner's computer and accesses or deletes her files. It is not clear whether the data would be considered restricted if, for example, she had shared her password with him.

Summary Offences Act 1966 (Vic)

See the ***Legal Guide to Image-Based Abuse in Vic*** for more information on intimate image offences.

14. Observation of genital or anal region (section 41A)

It is an offence for a person to intentionally observe, with the aid of a device, another person's genital or anal region in circumstances in which it would be reasonable for that person to expect that his or her genital or anal region could not be observed.

It does not matter that the other person (the person being observed) is in a public place when this offence occurs.

This is commonly known as the 'upskirting' offence.

Maximum penalty: Imprisonment for 3 months.

- ➢ **For example:** A woman wearing a skirt is walking up a staircase. A person walks behind the woman and uses a mirror to look under her skirt. This person has committed an offence.

Relevant exceptions (s 41D):

- if the other person has consented, expressly or impliedly, to the observation
- if the person making such an observation does so by accessing the Internet

15. Visually capturing genital or anal region (section 41B)

It is an offence for a person to intentionally visually capture another person's genital or anal region in circumstances in which it would be reasonable for that other person to expect that his or her genital or anal region could not be visually captured.

It does not matter that the other person (the person being visually captured) is in a public place when this offence occurs.

Maximum penalty: Imprisonment for 2 years.

Relevant exceptions (s 41D):

- if the other person has consented, expressly or impliedly, to the visual capture
- if the visual capturing is made by accessing the Internet

Note: This offence fills in a gap left by the *Surveillance Devices Act 1999* (Vic), which only covers the use of an optical surveillance device to record visually or observe a private activity (See ***Legal Guide to Surveillance Devices in Vic***).

16. Distribution of an image of genital or anal region (section 41C)

It is an offence for a person who has visually captured an image of another person's genital or anal region (whether or not in contravention of section 41B) to intentionally distribute that image.

Maximum penalty: Imprisonment for 2 years.

Relevant exceptions (s 41D):

- if the person the subject of the image expressly or impliedly consents to the distribution of the image for a particular purpose or a similar purpose
- if the subject is a child and the image was captured in contravention of section 41B and in the particular circumstances a reasonable person would regard the distribution of that image as acceptable

17. Distribution of intimate image (section 41DA)

It is an offence for a person ('A') to intentionally distribute an intimate image of another person ('B') to a person other than B, without B's express or implied consent to the distribution and manner of distribution, if the distribution of the image is contrary to community standards of acceptable conduct.

Maximum penalty: Imprisonment for 2 years.

➢ **For example:** A person posts a photograph of his ex-girlfriend engaged in sexual activity on a social media website without her express or implied consent.

18. Threat to distribute intimate image (section 41DB)

It is an offence for a person ('A') to make a threat to another person ('B') to distribute an intimate image of B or of another person ('C') and the distribution of the image would be contrary to community standards of acceptable conduct and A intends that B will believe, or believes that B will probably believe, that A will carry out the threat.

Maximum penalty: Imprisonment for 1 year.

Criminal Code 1995 (Cth)

19. 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).

20. 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.

21. 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 (section 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 (section 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 (section 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)

22. 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

23. 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).

24. 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

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**