AUSTRALIAN CAPITAL TERRITORY

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES IN THE AUSTRALIAN CAPITAL 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 Relevant Criminal Offences in the ACT

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 the ACT

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 Orders in the ACT

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

Legal Guide to Image-Based Abuse Legislation in the ACT

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 minor theft), are known as summary offences. Summary offences normally have a maximum penalty of no more than 2 years 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 2 years.

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 133 of the *Legislation Act 2001* (ACT) and increases with inflation. As of 2021, one penalty unit = $160 (for individuals). Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of $8,000.

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 ACT and Commonwealth laws that are relevant to technology-facilitated stalking and abuse.

Note: *The Listening Devices Act 1992* (ACT) and *Domestic Violence and Protection Orders Act 2008* (ACT) also contain relevant offences – these offences are covered in the **Legal Guide to Surveillance Legislation in the ACT** and the ***Legal Guide to Domestic Violence Orders in the ACT***. The intimate image offences contained in the *Crimes Act 1900* are dealt with in greater detail in the ***Legal Guide to Image-Based Abuse in the ACT***.

This guide covers the following legislation:

Criminal Code 2002 (ACT)

1. Blackmail (s 342)
2. Threat to cause property damage – fear of death or serious harm (s 406)
3. Threat to cause property damage (s 407)
4. Unauthorised access, modification or impairment with intent to commit serious offence (s 415)
5. Unauthorised modification of data to cause impairment (s 416)
6. Unauthorised impairment of electronic communication (s 417)
7. Unauthorised access to or modification of restricted data held in computer (s 420)

Crimes Act 1900 (ACT)

8. Threat to kill (s 30)
9. Threat to inflict grievous bodily harm (31)
10. Demands accompanied by threats (s 32)
11. Stalking (s 35)
12. Intimate observations or capturing visual data etc (s 61B)
13. Non-consensual distribution of intimate images (ss 72C and 72D)
14. Threat to capture or distribute intimate image (s72E)
15. Failure to comply with court order for rectification (s 72H)

Criminal Code 1995 (Cth)

16. Dealing in identification information (s 372.1)
17. Interception devices (s 474.4)
18. Offences using a carriage service
    a. To make a threat (s 474.15)
    b. To menace, harass or cause offence (s 474.17)

Telecommunications (Interception and Access) Act 1979 (Cth)

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

Criminal Code 2002 (ACT)

1. Blackmail (section 342)

It is an offence for a person to make an unwarranted demand with a menace of someone else with the intention of obtaining gain or causing loss. The demand does not need to be for money or other property.

Menace includes making an express or implied threat to of action that is detrimental or unpleasant to someone else. For the behaviour to be menacing it must be a threat that would be likely to cause a person of normal stability and courage to act unwillingly, or it would be likely to cause the individual to act unwillingly because of their particular vulnerability, known to the person making the threat.

Gain can be of property (whether temporary or permanent) or the supply of services and can also include keeping what one already has. A *loss* can mean a loss of property (whether temporary or permanent) (see s 300).

Maximum penalty: 1,400 penalty units or imprisonment for 14 years or both.

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

2. Threat to cause property damages – fear of death or serious harm (section 406)

It is an offence for a person to threaten to damage property where they are reckless about causing the threatened person to fear that if the threat were carried out, it would kill or cause serious harm to that person or another person. It is not necessary to prove that the threatened party actually feared the threat would be carried out.

Maximum penalty: 700 penalty units or imprisonment for 7 years or both.

- ➢ **For example:** a person sends his ex-partner a text message saying that he will burn her house down while she is sleeping.

3. Threat to cause property damages (section 407)

It is an offence for a person to threaten to damage property that belongs to another person where they intend for the threatened person to fear the threat will be carried out. It is not necessary to prove that the threatened party actually feared the threat would be carried out.

Maximum penalty: 200 penalty units or imprisonment for 2 years or both.

- ➢ **For example:** a person sends his ex-partner a text message saying that he will cut up all her clothes and burn her diary.

4. Unauthorised access, modification or impairment with intent to commit serious offence (section 415)

It is an offence if a person causes unauthorised access to or modification of data in a computer, or to cause unauthorised impairment of electronic communication to or from a computer, where that person knows it was unauthorised and they intend to commit or enable a serious offence (i.e. an offence punishable by imprisonment for 5 years or longer). It does not matter whether it is possible for the serious offence to be carried out.

Maximum penalty: the maximum penalty that would be applicable if the person had committed, or enabled the commission of, the serious offence.

- ➢ **For example:** a woman flees a domestic violence situation and is in hiding. The perpetrator infects her computer with spyware so can he can find out her new address and go there to assault her.

5. Unauthorised modification of data to cause impairment (section 416)

It is an offence if a person causes unauthorised modification of data held in a computer knowing the modification is unauthorised. The person must intend by the modification to impair access, reliability, security or the operation of data held in the computer, or be reckless about any such impairment. It does not matter whether there was any actual impairment caused.

Maximum penalty: 1,000 penalty units or imprisonment for 10 years or both.

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

6. Unauthorised impairment of electronic communication (section 417)

It is an offence if a person causes unauthorised impairment of electronic communication to or from a computer, knowing the impairment is unauthorised. The person must intend to impair electronic communication to or from the computer, or be reckless about any such impairment. The impairment must be more than mere interception of the communication.

Maximum penalty: 1,000 penalty units or imprisonment for 10 years or both.

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

7. Unauthorised access to or modification of restricted data held in computer (section 420)

It is an offence for a person to cause unauthorised access to or modification of *restricted data* held in a computer knowing it is unauthorised and intending to cause the access or modification.

Restricted data includes data restricted by an access control system, for example, where you need a password to log in to the computer. It is not clear whether the data would be considered restricted if, for example, the owner had shared her password with the perpetrator.

Maximum penalty: 200 penalty units or imprisonment for 2 years or both.

- ➢ **For example:** a person hacks in to his ex-partner's computer and accesses or deletes her files.

Crimes Act 1900 (ACT)

8. Threat to kill (section 30)

It is an offence to make a threat to another person to kill them or any third party, intending them to fear the threat will be carried out or being reckless to their fear. The threat must be in circumstances where a reasonable person would fear it would be carried out.

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 fears he will carry out his threat.

9. Threat to inflict grievous bodily harm (section 31)

It is an offence to make a threat to another person to inflict grievous bodily harm on them or any third party, intending them to fear the threat will be carried out or being reckless to their fear. The threat must be in circumstances where a reasonable person would fear it would be carried out.

Maximum penalty: imprisonment for 5 years.

- ➢ **For example:** a person sends his ex-partner a private message on social media stating how he plans to throw acid onto her and because of the history of domestic violence she fears he will carry out his threat.

10. Demands accompanied by threats (section 32)

Demands with threats to kill or cause grievous bodily harm

It is an offence for a person to make demands of another person with a threat to kill or inflict grievous bodily harm on a person.

Maximum penalty: imprisonment for 20 years.

- ➢ **For example:** a person calls his ex-partner and says if she doesn't allow him to see the children, he will kill her.

Demands with threats to endanger

It is an offence for a person to make demands of another person with a threat to endanger the health, safety or physical wellbeing of a person.

A threat to endanger a person's health, safety or physical wellbeing does not include threats to publish compromising photos of a person (*R v Butler* [2012] CTSC 124, 35).

Maximum penalty: imprisonment for 10 years.

➢ **For example:** a person calls his ex-partner and says if she doesn't get back together with him, he will send someone to her house to beat her up.

11. Stalking (section 35)

It is an offence for a person to stalk someone with intent to harm them, harass them or to cause them apprehension or fear of harm. Harm includes temporary or permanent physical or mental harm.

Stalking is where on at least two separate occasions a person does one or more of the following:

- Follows or approaches the stalked person
- Loiters near, watches, approaches or enters a place where the stalked person resides, works or visits
- Keeps the other person under surveillance
- Interferes with the property in possession of the stalked person
- Gives or sends offensive material to the other person, or leaves offensive material where it will be found by, given to or brought to the attention of the other person
- Telephones, sends electronic messages to or otherwise contacts the stalked person;
- Sends electronic messages about the stalked person to anybody else
- Makes electronic messages about the stalked person available to anybody else
- Acts covertly in a way that could reasonably be expected to arouse apprehension or fear in the stalked person
- Engages in conduct amounting to intimidation, harassment or molestation of the stalked person

Maximum penalty: imprisonment for 2 years. However, if the offence involved a contravention of an injunction or other court order (such as a FVO), or if the offender was in possession of an offensive weapon, then imprisonment for 5 years.

➢ **For example:** in *Scott William Longfield v Amanda Louise Glover* [2005] ACTSC 25 the court held that Longfield had been stalking and harassing his ex-partner Glover by ringing her at work, home and on her mobile, saying at one point, "I control your life".

12. Intimate observations or capturing visual data (section 61B)

Observing or capturing visual data where indecent or an invasion of privacy (section 61B(1))

It is an offence to observe another person with the aid of a device or to capture visual data of them where a reasonable person would find it to be indecent or an invasion of privacy in the circumstances.

It is a defence to this offence if the person can prove:

- They believed on reasonable grounds that the other person consented; or
- They did not know and could not reasonably be expected to have known, that it was without the other person's consent

Maximum penalty: 200 penalty units or imprisonment for 2 years or both.

➢ **For example:** setting up a surveillance camera in a woman's bedroom to observe her without her knowledge.

Observing or capturing visual of private region (section 61B(5))

It is an offence to observe another person with the aid of a device or to capture visual data of:

- Their genital or anal region; or

- The breasts of a female person or a transgender or intersex person who identifies as a female; and

where a reasonable person would find it to be an invasion of privacy in the circumstances.

It is a defence to this offence if the person can prove:

- They believed on reasonable grounds that the other person consented; or
- They did not know and could not reasonably be expected to have known, that it was without the other person's consent

Maximum penalty: 200 penalty units or imprisonment for 2 years or both.

➢ **For example:** using a mobile phone to take photos of a woman's underwear under her skirt or down the front of her blouse without her consent.

13. Non-consensual distribution of intimate image (section 72C)

Under this section, it is an offence to distribute an intimate image of another person knowing the other person does not consent, or being reckless as to whether the other person consents, to the distribution.

Maximum penalty: 300 penalty units or imprisonment for 2 years, or both.

➢ **For example:** A person receives a nude photograph of his partner sent by text message to his phone. He forwards the photograph to several friends without obtaining the consent of his partner. The person has committed an offence under this section.

Non-consensual distribution of intimate image of a young person (section 72D)

Under this section, it is an offence to distribute an intimate image of a person under the age of 16. It is a defence to this section to prove either:

- that the defendant reasonably believed the person of whom the image was taken was at least 16 years old; or
- that the image is of a person older than 10 years and not more than 2 years younger than the defendant, and that person consented to the distribution of the image.

Maximum penalty: 500 penalty units or imprisonment for 5 years, or both.

➢ **For example:** A 40 year-old person posts a photo of a naked 15 year-old person taking a shower to a website.

14. Threaten to capture or distribute intimate image (section 72E)

It is an offence to threaten to capture or distribute an intimate image of another person while intending the other person fear, or being reckless as to whether the other person fears, that the threat will be carried out.

A threat may be made by any conduct, whether explicit or implicit, conditional or unconditional. It is not necessary to prove that the other person actually feared the threat would be carried out, or even that carrying out the threat was possible (for example, if the image does not exist).

Maximum penalty: 300 penalty units or imprisonment for 3 years, or both.

➢ **For example:** A person tells his partner that she must perform certain sexual acts for him, and that if she refuses, he will post a video he has recorded of the two of them having sex to her Facebook page. The person has committed an offence under this section, regardless of whether he has in fact recorded such a video or plans to share it.

15. Failure to comply with court order rectification (Section 72H)

A court that finds a person guilty of an offence against sections 72C, 72D or 72E may order the person to take reasonable action to remove, retract, recover, delete or destroy an intimate image involved in the offence within a stated period.

It is an offence to fail to comply with such an order.

Maximum penalty: 200 penalty units or imprisonment for 2 years, or both.

➢ **For example:** A person has been found guilty of an offence against section 72C for posting naked photographs of his girlfriend to a range of websites. The court orders the defendant to destroy the photographs, and, within two weeks, to contact every website on which the photographs are hosted and request that they be removed. After two weeks, the defendant has failed to destroy the photos or contact the websites. He has committed an offence under this section.

Criminal Code 1995 (Cth)

16. 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).

17. 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.

18. 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)

19. 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.

20. 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).

21. 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
- 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**