NEW SOUTH WALES

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES IN NEW SOUTH WALES

Introduction

Technology-facilitated stalking and abuse is the use of technology (such as the internet, social media, mobile phones, computers, and surveillance devices) to stalk and perpetrate abuse on a person.

Such behaviour includes:

- Making numerous and unwanted calls to a person's mobile phone
- Sending threatening and/or abusive messages (text messaging, WhatsApp, Snapchat, Facebook messaging, Twitter)
- Hacking into a person's email or social media account to discover information about them
- Hacking into a person's email or social media account to impersonate them and send abusive messages to family/friends of that person
- Using surveillance devices to spy on a person
- Using tracking devices to follow a person
- Sharing, or threatening to share, intimate pictures of a person

This legal guide is one of a set of four guides that looks at areas of law relevant to people experiencing technology-facilitated stalking and abuse.

Legal Guide to Relevant Criminal Offences in NSW

This guide looks at the various criminal offences that may apply to a person who is perpetrating technology-facilitated stalking and abuse.

For information on other areas of law see:

Legal Guide to Surveillance Legislation in NSW

This guide looks at what the law says about surveillance devices – when it is an offence to use them and what the restrictions are on sharing information/videos/pictures obtained through the use of surveillance devices.

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

Legal Guide to Image-based Abuse in NSW

This guide looks at what the law says about image-based abuse – when it is an offence to record or distribute intimate images and what legal options exist for victims of image-based abuse.

Language

‘Victim’ vs. ‘Survivor’

Some women who are experiencing, or who have experienced, domestic violence use the term ‘victim’ of domestic violence to describe themselves. Others believe the term ‘survivor’ of domestic violence more accurately reflects their experience. Whilst acknowledging that each woman’s experience is unique and individual to her circumstances, for consistency, these guides will refer to women who are experiencing, or who have experienced, domestic violence as ‘victim-survivors’ of domestic violence.

Gender

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

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 NSW and Commonwealth law that are relevant to technology-facilitated stalking and abuse.

Note: *The Surveillance Devices Act 2007* (NSW) and *Crimes (Domestic and Personal Violence) Act 2007* (NSW) also contain relevant offences – these offences are covered in the ***Legal Guide to Surveillance Legislation in NSW*** and the ***Legal Guide to Apprehended Domestic Violence Orders in NSW***. The intimate image offences contained in sections 91P - 91S of the *Crimes Act 1900* (NSW) are covered in greater detail in the ***Legal Guide to Image-Based Abuse in NSW***.

This guide covers the following legislation:

Crimes Act 1900 (NSW)

1. Documents containing threats (s 31)
2. Voyeurism (s 91J)
3. Filming a person engaged in a private act (s 91K)
4. Filming a person's private parts (s 91L)
5. Installing device to facilitate observation or filming (s 91M)
6. Recording an intimate image without consent (91P)
7. Distributing an intimate image without consent (91Q)
8. Threatening to record or distribute an intimate image (91R)
9. Contravening a court order for rectification following a conviction under ss 91P or 91Q (91S)
10. Blackmail offence (s 249K)
11. Unauthorised access, modification or impairment with intent to commit serious indictable offence (s 308C)
12. Unauthorised access to or modification of restricted data held in computer (s 308H)
13. Publishing indecent articles (s 578C)

Criminal Code 1995 (Cth)

14. Dealing in identification information (s 372.1)
14. Interception devices (s 474.4)
16. 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)

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

Crimes Act 1900 (NSW)

1. Documents containing threats (section 31)

It is an offence for a person, knowing the document's contents, to intentionally or recklessly send, deliver, or directly or indirectly cause to be received, any document threatening to kill or inflict bodily harm on any person.

Maximum penalty: Liable to 10 years imprisonment.

➢ **For example:** sending a message (email, text messaging, Whatsapp, Snapchat, Facebook messaging, Twitter) threatening to kill or hurt someone.

2. Voyeurism (section 91J)

It is an offence to observe a person, without the person's consent or knowing that the person has not consented, engaging in a private act for the purpose of obtaining sexual arousal or gratification.

Maximum penalty: Imprisonment for 2 years or a fine of 100 penalty units, or both.

A person is *engaged in a private act* if:

- the person is in a state of undress, using the toilet, showering or bathing, engaged in a sexual act of a kind not ordinarily done in public, or engaged in any other like activity; and
- the circumstances are such that a reasonable person would reasonably expect to be afforded privacy.

3. Filming a person engaged in a private act (section 91K)

It is an offence to *film another person who is engaged in a private act*, without the person's consent or knowing that the person has not consented, for the purpose of obtaining or enabling another person to obtain sexual arousal or sexual gratification.

Maximum penalty: Imprisonment for 2 years or a fine of 100 penalty units, or both.

➢ **For example:** where a sex-tape is filmed without one or both parties' consent for the purpose of uploading to a pornographic website.

If the offender constructs or adapts the fabric of any building to facilitate the filming of a person engaged in a private act, this is considered a circumstance of aggravation and the offender can be charged with an aggravated offence with a maximum penalty of imprisonment for five years.

Maximum penalty: Imprisonment for 5 years.

➢ **For example:** A person drills holes into the ceiling and walls of his bedroom to hide video cameras so that he can film himself have sex with his girlfriend, knowing that his girlfriend has not consented to him filming them having sex.

4. Filming a person's private parts (section 91L)

It is an offence to film another person's private parts, without the person's consent or knowing that the person has not consented, in circumstances in which a reasonable person would reasonably expect not to be filmed, for the purpose of obtaining or enabling another person to obtain sexual arousal or sexual gratification.

Maximum penalty: Imprisonment for 2 years or a fine of 100 penalty units, or both.

➢ **For example:** placing a video camera in a bathroom to film another person, without that person's consent, getting in and out of the shower.

If the offender constructs or adapts the fabric of any building to facilitate the filming of a person's private parts, this is considered a circumstance of aggravation and the offender can be charged with an aggravated offence.

Maximum penalty: Imprisonment for 5 years.

➢ **For example:** a person drills holes into the walls of a bathroom to hide video cameras so that he can film a family member using the shower, knowing that the person has not consented to him doing so.

Note: A person cannot be convicted of both a section 91K offence and a section 91L offence for the same conduct that occurred on a particular occasion (the 'double jeopardy' provision).

5. Installing device to facilitate observation or filming (section 91M)

It is an offence for a person, with the intention of enabling himself or another person to commit an offence against sections 91J, 91K or 91L, to install a device, construct or adapt the fabric of any building in order to facilitate the observation or filming of another person.

Maximum penalty: Imprisonment for 2 years or a fine of 100 penalty units, or both.

If offences against sections 91J, 91K or 91L are not proven, this offence may be relied upon as an alternative verdict.

6. Recording an intimate image without consent (section 91P)

It is an offence to intentionally record an intimate image of another person without the consent of the person, and knowing the person did not consent to the recording or being reckless as to whether the person consented to the recording.

Maximum penalty: 100 penalty units or imprisonment for 3 years, or both.

- **For example:** a person hides a camera in a bedroom and films a sexual encounter between himself and a partner, without obtaining the partner's consent.

7. Distributing an intimate image without consent (section 91Q)

It is an offence to intentionally distribute an intimate image of another person without the consent of the person, and knowing the person did not consent, or being reckless as to whether the person consented, to the distribution.

Maximum penalty: 100 penalty units or imprisonment for 3 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.

8. Threatening to record or distribute an intimate image (section 91R)

It is an offence to threaten to record or distribute an intimate image of another person without the consent of the other person, and intending to cause that other person to fear that the threat will be carried out.

Maximum penalty: 100 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.

9. Contravening a court order for rectification following a conviction under sections 91P or 91Q (section 91S)

A court that finds a person guilty of an offence against section 91P or 91Q may order the person to take reasonable actions to remove, retract, recover, delete or destroy any intimate image recorded or distributed by the person in contravention of the section within a period specified by the court.

A person who, without a reasonable excuse, contravenes an order made under this section is guilty of an offence.

Maximum penalty: 50 penalty units or imprisonment for 2 years, or both.

- **For example:** a person has been found guilty of an offence against section 91Q 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.

For more information on the offences outlined in sections 91P – 91S, including definitions and exemptions, and other image-based abuse offences, see the ***Legal Guide to Image-Based Abuse in NSW***.

10. Blackmail (section 249K)

It is an offence for a person to make an unwarranted demand with menaces with the intention of obtaining a gain or causing a loss.

Maximum penalty: Imprisonment for 10 years.

➢ **For example:** A person threatens to release intimate pictures of his ex-girlfriend to her family unless she gives him half of her monthly salary.

11. Unauthorised access to or modification of restricted data held in computer (section 308H)

It is an offence for a person to intentionally cause any unauthorised access to or modification of restricted data held in a computer, knowing that the access or modification is unauthorised. Data is restricted when it is, for example, protected by a password.

Maximum penalty: Imprisonment for 2 years.

Although the maximum penalty for this offence is 2 years imprisonment, this offence is considered a summary offence.

➢ **For example:** a person hacks a woman's computer to download intimate pictures she has of herself.

12. Unauthorised access, modification or impairment with intent to commit serious indictable offence (section 308C)

It is an offence for a person, knowing it is unauthorised, to:

- access data held in any computer, or
- modify data held in any computer, or
- impair electronic communication to or from any computer

with the intention of committing a serious indictable offence, or facilitating the commission of a serious indictable offence (whether by the person or by another person).

Maximum penalty: The maximum penalty applicable if the person had committed, or facilitated the commission of, the serious indictable offence in this jurisdiction.

➢ **For example:** a person hacks into his ex-girlfriend's computer to obtain intimate pictures she has of herself in order to blackmail her into giving him half of her monthly salary.

13. Publishing indecent articles (section 578C)

It is an offence for a person to publish an indecent article.

Maximum penalty: Imprisonment for 12 months or a fine of 100 penalty units, or both.

➢ **For example:** a man posted nude photographs of his ex-girlfriend on his Facebook account. He then requested, through Facebook, to be friends with the victim's relatives in order to show them the photographs. He was charged with and found guilty of an offence under s 578C. (*Police v Ravshan Usmanov* [2011] NSWLC 40).

Criminal Code 1995 (Cth)

14. 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 section 474.17).

15. 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.

16. 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 video conference calls.

Telecommunications (Interception and Access) Act 1979 (Cth)

17. 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

18. 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).

19. 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**