QUEENSLAND

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES IN QUEENSLAND

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 QLD

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 QLD

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 Domestic Violence Protection Orders in QLD

This guide looks at how people can obtain protection orders from the court to protect them from technology-facilitated stalking and abuse. In Queensland these protection orders are called **domestic violence protection orders (DVOs)**.

Legal Guide to Image-Based Abuse Legislation in QLD

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 a 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 Penalties and Sentences Regulation 2015 (QLD) states the dollar amount for one penalty unit. As of 1 July 2021, one penalty unit = $137.00. Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of $6,850.00.

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

Note: *The Invasion of Privacy Act 1971* (Qld) and *Domestic and Family Violence Protection Act 2012* (Qld) also contain relevant offences – these offences are covered in the ***Legal Guide to Surveillance Legislation in QLD*** and the ***Legal Guide to Domestic Violence Protection Orders in QLD***. The observation and recording offences contained in the *Criminal Code 1899* (Qld) are dealt with in greater detail in the ***Legal Guide to Image-Based Abuse in QLD***.

This guide covers the following legislation:

Criminal Code 1899 (Qld)

1. Observations or recordings in breach of privacy (s 227A)
2. Distributing prohibited visual recordings (s 227B)
3. Obscene publications and exhibitions (s228)
4. Punishment of unlawful stalking (s 359E)
5. Computer hacking and misuse (s 408)
6. Extortion (s 415)

Criminal Code 1995 (Cth)

7. Dealing in identification information (s 372.1)
8. Interception devices (s 474.4)
9. 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)

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

Criminal Code 1899 (Qld)

1. Observations or recordings in breach of privacy (section 227A)

In a private place or engaged in a private act: section 227A(1)

It is an offence for a person (person A) to observe or visually record another person (person B) without person B's consent and in circumstances where a reasonable adult would expect to be afforded privacy, when:

- person B is in a private place; or
- person B is engaging in a private act and the observation or visual recording is made for the purpose of observing or visually recording a private act

Circumstances where a reasonable adult would expect to be afforded privacy:

- A person changing in a communal change room at a swimming pool may expect to be observed by another person who is also changing in the room but may not expect to be visually recorded.
- A person who needs help to dress or use a toilet may expect to be observed by the person giving the help but may not expect to be observed by another person.

Maximum penalty: Imprisonment for 3 years.

➢ **For example:** Installing a camera in a bathroom to film a person using it (*R v VAB* [2014] QDC 113).

A person's genital or anal region: section 227A(2)

It is also an offence for a person (person A) to observe or visually record another person (person B's) genital or anal region without person B's consent and in circumstances where a reasonable adult would expect to be afforded privacy in relation to that region, when the observation or visual recording is made for the purpose of observing or visually recording person B's genital or anal region.

Maximum penalty: Imprisonment for 3 years.

➢ **For example:** Using a mobile phone in a public place to take photos of women's underwear under their skirts without their consent.

2. Distributing prohibited visual recordings (section 227B)

A visual recording made in contravention of section 227A (above) is a *prohibited visual recording*.

It is an offence for a person (person A) to distribute a prohibited visual recording of another person (person B), when person A has reason to believe that it is a prohibited visual recording and person A does not have person B's consent.

Maximum penalty: Imprisonment for 3 years.

See section 227B of the *Criminal Code* for the meaning of 'distribute'.

3. Obscene publications and exhibitions (section 228)

It is an offence for a person to knowingly, and without lawful justification or excuse, publicly sell, distribute or expose for sale:

- any obscene book or obscene printed or written matter
- any obscene computer-generated image
- any obscene picture, photograph, drawing, or model
- any other object tending to corrupt morals

It is also an offence for a person to knowingly, and without lawful justification or excuse, expose to view in any place to which the public are permitted to have access:

- any obscene picture, photograph, drawing, or model
- any other object tending to corrupt morals

Maximum penalty: Imprisonment for 2 years.

4. Unlawful stalking (sections 359A–E)

It is an offence for a person to unlawfully stalk another person (s 359E).

Maximum penalty: Imprisonment for 5 years.

It is a more serious offence if a person unlawfully stalks another person and:

- uses, or intentionally threatens to use, violence against anyone or anyone's property; or
- possesses a weapon.

In such a case, the maximum penalty is imprisonment for seven years.

Unlawful stalking has a very specific meaning, defined in section 359B of the *Criminal Code*.

Four elements make up the offence of *unlawful stalking*:

1. It is intentionally directed at a person ('stalked person' / 'aggrieved').
2. It is engaged in on more than one occasion. Or, if the conduct lasts for a long time, it is engaged in on any one occasion.
3. It consists of one or more particular behaviours (see below).
4. it causes the aggrieved person detriment reasonably arising in the circumstances.

Particular behaviours related to technology-facilitated stalking:

- following, loitering near, watching or approaching a person;
- contacting a person in any way, including, for example, by telephone, mail, fax, email or through the use of any technology
- leaving offensive material where it will be found by, given to or brought to the attention of, a person (eg, posting offensive material on the aggrieved person's Facebook wall)
- giving offensive material to a person, directly or indirectly (eg, emailing offensive pictures to the aggrieved person)
- an intimidating, harassing or threatening act against a person, whether or not involving violence or a threat of violence
- an act of violence, or a threat of violence, against, or against property of, anyone, including the respondent

Detriment may include the following:

- apprehension or fear of violence to, or against property of, the aggrieved or another person
- serious mental, psychological or emotional harm
- prevention or hindrance from doing an act a person is lawfully entitled to do
  - For example, a person no longer walks outside the person's place of residence or employment or a person significantly changes the route or form of transport the person would ordinarily use to travel to work or other places
- compulsion to do an act a person is lawfully entitled to abstain from doing
  - For example, a person sells a property the person would not otherwise sell

A court may also make a restraining order in relation to this offence. See section 359F for more information.

5. Computer hacking and misuse (section 408E)

It is an offence for a person to use a restricted computer (password protected) without the consent of the person who controls the computer.

Maximum penalty: Imprisonment for 2 years.

The maximum penalty increases to imprisonment for 10 years if the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit.

➢ **For example:** A person hacks into his ex-partner's computer in order to obtain personal or sensitive information about her.

6. Extortion (section 415)

It is an offence for a person ('the demander') to demand something of another person without reasonable cause, when the demand is accompanied by a threat to cause a detriment to any person other than the demander, and the demander has the intention of gaining a benefit for any person or causing a detriment to any person other than the demander.

Maximum penalty: Imprisonment for 14 years, unless the carrying out of the threat causes or would be likely to cause substantial economic loss or serious personal injury to a person other than the offender, in which case, life imprisonment.

- ➢ **For example:** Where a person threatens to release a sex tape of his ex-partner if she does not meet his demand to return to the relationship or to give him a sum of money.

The *Criminal Code* defines 'benefit' to include property, advantage, service, entertainment, the use of or access to property or facilities, and anything of benefit to a person whether or not it has any inherent or tangible value, purpose or attribute (See section 1).

Criminal Code 1995 (Cth)

7. 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).

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).

This is commonly referred to as 'identity fraud'.

8. 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.

9. 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)

10. 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

11. 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).

12. 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