TASMANIA

VERSION 3.0

Women's technology safety

Legal Guides

LEGAL GUIDE TO RELEVANT CRIMINAL OFFENCES IN TASMANIA

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 TAS

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 TAS

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 TAS

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

Legal Guide to Image-Based Abuse Legislation in TAS

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

Language of '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 and Language

While domestic violence can happen in many circumstances (including in non-heterosexual relationships), in the vast majority of reported domestic violence cases men are the people perpetrating the abuse and women are the victim-survivors. For this reason these guides use 'he' to refer to perpetrators and 'she' to refer to victims. This is not intended to exclude other situations.

Terminology

Criminal offence (or offence)

A criminal offence is an offence against the State. It is commonly referred to as 'breaking the law'.

Summary offence

Less serious offences (such as obscenity or loitering), are known as summary offences. Summary offences are dealt with by the Magistrates Court.

Indictable offence

More serious offences (such as murder, manslaughter, sexual assault) are known as indictable offences and are usually dealt with by the Supreme Court.

Charge

When a person is charged with an offence, it means that the police have formally accused that person of committing an offence.

Conviction

When a person is convicted of an offence, it means that person has either pleaded guilty to committing the offence, or a court has found that person guilty of committing the offence.

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 *Penalty Units and Other Penalties Act 1987* (Tas) states the dollar amount for one penalty unit. As of July 2021: one penalty unit = $173. Therefore, an offence with a maximum penalty of a fine of 50 penalty units will have a maximum fine of $8,650.

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

Note: Other relevant offences are contained in the *Listening Devices Act 1991* (Tas), the *Family Violence Act 2004* (Tas). These offences are covered in the ***Legal Guide to Surveillance Legislation in TAS*** and the ***Legal Guide to Family Violence Orders in TAS***. The observation and recording offences contained in the *Police Offences Act 1935* are dealt with in greater detail in the ***Legal Guide to Image-Based Abuse in TAS***.

This guide covers the following legislation:

Police Offences Act 1935 (Tas)

1. Observation or recording in breach of privacy (section 13A)
2. Publishing or distributing prohibited visual recording (section 13B)
3. Possession of prohibited visual recording (section 13C)
4. Damaging computer data (section 43B)
5. Unauthorised access to a computer (section 43C)
6. Insertion of false information as data (section 43D)

Criminal Code Act 1924 (Tas)

7. Written threats to murder (section 162)
8. Stalking (section 192)
9. Damaging computer data (section 257C)
10. Unauthorised access to a computer (section 257D)
11. Threats to destroy property (section 276)
12. False threats of danger (section 276AA)

Criminal Code 1995 (Cth)

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

Telecommunications (Interception and Access) Act 1979 (Cth)

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

Police Offences Act 1935 (Tas)

1. Observation or recording in breach of privacy (section 13A)

Observation/recording of private place or private act

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

- when B is in a private place; or
- when 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.

Maximum penalty: Fine not exceeding 50 penalty units or imprisonment for a term not exceeding 12 months, or both.

➢ **For example:** A person hides a video camera in his partner's bedroom, without her consent, for the purpose of visually recording her engaged in a private act.

'Upskirting' offence

It is an offence for a person to observe or visually record another person's genital or anal region, in circumstances where a reasonable person would expect privacy when the observation or visual recording is made for the purpose of observing or visually recording the other person's genital or anal region.

Maximum penalty: Fine not exceeding 50 penalty units or imprisonment for a term not exceeding 12 months, or both.

➢ **For example:** Using a mobile phone to take photographs under women's skirts.

2. Publishing or distributing prohibited visual recording (section 13B)

It is an offence for a person to publish or distribute a prohibited visual recording of another person having reason to believe it to be a prohibited visual recording, without a lawful and reasonable excuse.

The onus is on the person who is alleged to have committed the offence to prove that the publication/distribution was done with a lawful and reasonable excuse.

Maximum penalty: Fine not exceeding 50 penalty units or imprisonment for a term not exceeding 12 months, or both.

➢ **For example:** It is an offence for a person to publish on Facebook nude pictures of his ex-partner, when she would have expected the pictures to be kept private between them.

Definitions

'Distribute' means communicate, exhibit, send, supply, transmit or make available to someone. Any attempt to distribute, or agreement or arrangement to distribute, will also be treated as an offence.

'Prohibited visual recording' means any visual recording of a person taken in a private place or engaging in a private act, or of a person's genital or anal region, whether covered only by underwear or bare, where a reasonable adult would expect to be afforded privacy.

3. Possession of prohibited visual recording (section 13C)

It is an offence for a person to be in possession of a prohibited visual recording, having reason to believe it to be a prohibited visual recording.

Maximum penalty: Fine not exceeding 50 penalty units or imprisonment for a term not exceeding 12 months, or both.

4. Damaging computer data (section 43B)

It is an offence for a person to, intentionally and without lawful excuse, destroy, damage, erase or alter data stored in a computer or interfere, interrupt or obstruct the lawful use of a computer, a system of computers or any part of it.

Maximum penalty: Fine not exceeding 20 penalty units or imprisonment for a term not exceeding two years, or both.

5. Unauthorised access to a computer (section 43C)

It is an offence for a person, without lawful excuse, to intentionally gain access to a computer, system of computers or any part of a system of computers.

Maximum penalty: Fine not exceeding 20 penalty units or imprisonment for a term not exceeding two years, or both.

6. Insertion of false information as data (section 43D)

It is an offence for a person to dishonestly introduce into, or record or store in, a computer or system of computers, by any means, false or misleading information as data.

Maximum penalty: Fine not exceeding 20 penalty units or imprisonment for a term not exceeding two years, or both.

Note: For the following offences:

- Damaging computer data (section 43B)
- Unauthorised access to a computer (section 43C)
- Insertion of false information as data (section 43D)

if a person does an act or thing referred to outside, or partly outside, Tasmania and there is a real and substantial link between doing the act or thing and Tasmania, these sections apply in relation to that act or thing as if it had been done wholly within Tasmania. See section 43E of the *Police Offences Act 1935* (Tas).

There is a '*real and substantial link*' with Tasmania if:

- a significant part of the conduct relating to, or constituting, the doing of the act or thing occurred in Tasmania; or
- where the act or thing was done wholly outside Tasmania or partly within Tasmania, if substantial harmful effects arose in Tasmania.

Criminal Code Act 1924 (Tas)

Note: The maximum penalty for all crimes under the *Criminal Code Act 1924* (Tas), other than murder and treason, and subject to the provisions of the *Sentencing Act 1997* (Tas), is imprisonment for 21 years (see Section 389). Courts exercise discretion in sentencing and sentences are rarely as long as 21 years in practice (See *Sentencing Advisory Council* (Tas) (https://www.sentencingcouncil.tas.gov.au/).

7. Written threats to murder (section 162)

It is an offence to make a written threat to kill a person with intent to intimidate or influence them.

➢ **For example:** a person sends their ex-partner a text message saying "I will kill you" to scare them.

8. Stalking (section 192)

It is an offence to do one or more of the following actions with intent to cause a person physical or mental harm or to be apprehensive or fearful:

- Following the other person or a third person;
- Keeping the other person or a third person under surveillance;
- Loitering outside the residence or workplace of the other person or a third person;

- Loitering outside a place that the other person or a third person frequents;
- Entering or interfering with the property of the other person or a third person;
- Sending offensive material to the other person or a third person or leaving offensive material where it is likely to be found by, given to or brought to the attention of the other person or a third person;
- Publishing or transmitting offensive material by electronic or any other means in such a way that the offensive material is likely to be found by, or brought to the attention of, the other person or a third person;
- Using the internet or any other form of electronic communication in a way that could reasonably be expected to cause the other person to be apprehensive or fearful;
- Contacting the other person or a third person by postal, telephonic, electronic or any other means of communication;
- Acting in another way that could reasonably be expected to cause the other person to be apprehensive or fearful

➢ **For example:** a person sends another person a large volume of harassing emails each day over a week

9. Damaging computer data (section 257C)

It is an offence to intentionally and without lawful excuse:

- Destroy, damage, erase or alter data stored in a computer; or
- Interfere with, interrupt or obstruct the use of a computer.

10. Unauthorised access to a computer (section 257D)

It is an offence to intentionally gain access to a computer without lawful excuse.

➢ **For example:** using spyware that allows a person to access another person's computer files and see their screen

11. Threats to destroy property (section 276)

It is an offence to directly or indirectly cause a person to receive a written threat to burn, destroy, or injure property.

➢ **For example:** sending a person an instant message that says "I will burn your house down"

12. False threats of danger (section 276AA)

It is an offence to make a false statement, knowing it is false, where it could be reasonably inferred some act will or is likely to be done, that would put persons or property at a serious risk of danger.

➢ **For example:** a man posts his ex-partner's name, photo and address on a forum pretending to be her and asking men to come to her house for rough sex, instructing "I will say no, but I mean yes, it's a part of the game".

Criminal Code 1995 (Cth)

13. Dealing in identification information (section 372.1)

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

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'.

14. Interceptions devices (section 474.4)

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

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

Maximum penalty: Imprisonment for 5 years.

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

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

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

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

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

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

Maximum penalty: Imprisonment for 10 years.

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

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

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

Maximum penalty: Imprisonment for 7 years.

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

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

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

Maximum penalty: Imprisonment for 3 years.

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

Telecommunications (Interception and Access) Act 1979 (Cth)

16. Interception of telecommunications (section 7)

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

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

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

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

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

17. Dealing in intercepted information (section 63)

A person must not communicate to another person, make use of, or make a record of, or give evidence in a proceeding any information that has been intercepted (subject to the other provisions of Part 2-6).

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

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

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

Some orders the court can make are:

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

Online Safety Act 2021 (Cth)

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

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

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

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

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

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

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

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

Gathering evidence to prove technology-facilitated stalking or abuse

Sometimes it can be difficult to prove technology-facilitated stalking or abuse. Some tips for gathering evidence to show that technology-facilitated stalking or abuse has occurred are:

- Do not delete text messages, voicemail messages, photos
- Try and save any evidence to a computer/USB flash drive
- Use screenshots and save the image as the date & time it was taken. If taking screenshots of websites, always include the URL in the screenshot
- Keep a diary or voice notes of incidents including dates and times
- Consider giving police written permission to access your phone, computer, Facebook, email account etc. if a matter is being investigated

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**