

LEGAL GUIDE TO IMAGE-BASED ABUSE LEGISLATION IN WESTERN AUSTRALIA

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 Image-Based Abuse Legislation in WA

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.

For information on other areas of law see:

Legal Guide to Surveillance Legislation in WA

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 Relevant Criminal Offences in WA

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

Legal Guide to Family Violence Restraining Orders in WA

This guide looks at how people can obtain protection orders from the court to protect them from technology facilitated stalking and abuse. In Western Australia, these protection orders are called Family Violence Restraining Orders (FVROs).

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 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. Indictable offences are heard by the District Court or 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.

IMAGE-BASED ABUSE

Image-based abuse occurs when a nude, sexual or otherwise intimate image is taken or shared without the consent of the person featured in the image. It can also include the threat to share such an image whether or not the image is in fact shared, or whether or not the image in question even exists.

Image-based abuse is often referred to as “revenge porn”. This term is inaccurate, as in many cases the sharing or threat to share an intimate image is not motivated by ‘revenge’, and similarly the image need not be ‘pornographic’ to be intimate and private. Image-based abuse can occur for a wide range of motives, such as a desire to control, punish, humiliate or otherwise harm the victim, financial incentives, a desire for social status or notoriety or many others, and can include many different kinds of videos or images.

This guide focuses on the image-based abuse of adults. The production, possession and distribution of “child exploitation material” are criminal offences in Western Australia subject to a maximum penalty of imprisonment for 10 years. “Child exploitation material” includes but is not limited to material which depicts, describes or represents a person who is, or who appears to be, under 16, engaged in sexual activity, or in a sexual or otherwise demeaning context (*Criminal Code Compilation Act 1913* (WA) Chapter XXV). Some regulations of similar material exist in the *Criminal Code 1995* (Cth) (Divisions 273, 471B, 474D).

IMAGE-BASED ABUSE LEGISLATION IN WESTERN AUSTRALIA

At the time of publication, there are no criminal laws specifically governing image-based abuse in Western Australia.

Restraining Orders Act 1997 (WA)

Section 10G(2) of the *Restraining Orders Act 1997* (WA) sets out a range of orders that a court may make (but is not limited to), in order to restrain the behaviour of a defendant in family violence restraining order (FVRO) proceedings. These include:

- distributing or publishing, or threatening to distribute or publish, intimate personal images of the person seeking to be protected, and
- causing or allowing another person to engage in such conduct.

No further definition of “intimate personal images” is provided by the Act.

Breach of an FVRO is a criminal offence under section 61 of the *Restraining Orders Act 1997*.

Maximum penalty: A fine of \$6,000 or imprisonment for 2 years, or both.

- **For example:** A woman applies to court for a FVRO against her ex-partner. He was physically and sexually abusive toward her during their relationship. Since the relationship ended, he has been making various threats against her, including a threat to send nude photos he took of her during their relationship to her friends and family. The court grants an FVRO that includes the order under subsection 10G(2)(f) above. Her ex-partner continues to threaten to send the images to her friends and family after the order has been made. He has committed an offence under section 61 of the *Restraining Orders Act 1997* (WA).

Criminal Code 1995 (Cth)

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

A carriage service is defined in section 7 of the *Telecommunications Act 1997* (Cth) as a service for carrying communications by means of guided and/or unguided electromagnetic energy. It includes:

- telephone services
- internet access services, and
- Voice over Internet Protocol services eg. Skype)

Under section 474.17 it is an offence 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.

Private sexual material (Section 473.1)

This is defined as material that depicts a person who is, or appears to be, at least 18 years old and is engaged in, or appears to be in, a sexual pose or sexual activity in circumstances in which reasonable persons would have an expectation of privacy.

It also includes material that predominantly depicts a sexual organ or the anal region of a person who is, or appears to be, at least 18 years old or the breasts of a female person who is, or appears to be, at least 18 years old, in circumstances in which reasonable persons would have an expectation of privacy.

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.

The Act requires industry to develop new codes to regulate illegal and restricted content. The content that can be removed refers to the seriously harmful material including content that includes nudity and violence. Therefore it prohibits the non-consensual sharing or threatened sharing of intimate images.

Intimate image (Section 15)

Material is considered an intimate image of a person if it is a depiction of private parts:

- It can be still or moving images
- Depicts or appears to depict the person's genital area or anal area (bare or covered by underwear) or if, the person is a female or a transgender or intersex person identifying as female, either or both of the person's breasts in circumstances in which an ordinary reasonable person would expect privacy

Material is considered an intimate image of a person if it is a depiction of private activity:

- It can be still or moving images
- Depicts or appears to depict the person in a state of undress, using the toilet, showering, having a bath, engaged in a sexual act of a kind not ordinarily done in public or engaged in any other like activity in circumstances in which an ordinary reasonable person would expect privacy

Material is considered an intimate image of a person if it is a depiction of a person without attire of religious or cultural significance:

- It can be still or moving images
- Because of the person's religious or cultural background, the person consistently wears particular attire of religious or cultural significance whenever they are in public
- The image depicts or appears to depict the person without that attire and in circumstances in which an ordinary reasonable person would expect privacy

Non consensual intimate image of a person (Section 16)

If an intimate image of a person is provided on a social media service (s13), a relevant electronic service (s13A) or a designated internet service (s14) and the person did not consent to the image being shared on that service then the intimate image is a non-consensual image of the person.

Consent (Section 21)

Consent must be express, voluntary and informed. It does not include consent given by a child or by an adult who is in a mental or physical condition (temporary or permanent) that makes them incapable of giving consent or substantially impairs their capacity to give consent.

Posting an Intimate Image (Section 75)

A person must not post, or make a threat to post, an intimate image of another person online (on a social media service, relevant electronic service or designated internet service) if either they or the person photographed is ordinarily a resident in Australia.

Maximum penalty: 500 penalty units.

The elements of the offence are not met where consent to the posting of the image by the first person was given.

It is also not an offence if the intimate images depicts or appears to depict an individual without a particular piece of clothing of religious or cultural significance and the perpetrator did not know that, due to the other person's religious or cultural background, they consistently wore that piece of clothing whenever they were in public.

The eSafety Commissioner may issue a formal warning if a person contravenes s75 (s76).

- **For example:** A man posts nudes of his ex-partner on his Instagram account after they separate. He posts these up without her consent. The man has committed an offence under section 75.

Complaints (Section 32)

If a person has reason to believe that s75 has been contravened with respect to an intimate image of themselves or someone on whose behalf they are authorised to act, the person may lodge a complaint with the eSafety Commissioner. If they are not able to identify the alleged perpetrator, they must state this in their complaint.

Objection notice (Section 33)

If a person has reason to believe that an intimate image of themselves or someone on whose behalf they are authorised to act, has been provided online (a social media service, relevant electronic service or a designated internet service by an end-user) the depicted individual may lodge an objection notice with the eSafety Commissioner, regardless of whether they consented to the original posting of the image.

Removal notice given to the provider of a social media service, relevant electronic service or designated internet service OR to an end-user (Section 77 and 78)

If an individual made a complaint or objection notice under s32 or s33 and the relevant image was non-consensually posted online (by an end-user or a social media service, relevant electronic service or a designated internet service) the Commissioner may issue a written notice to the service provider or the end user. This removal notice will require that all reasonable steps be taken to ensure the removal of the intimate image from the service and to do so within 24 hours, or longer if the Commissioner allows.

If the relevant image is hosted by a hosting service provider, the Commissioner may give the hosting service provider a written notice to take reasonable steps to cease the hosting of the image (s79).

Compliance with removal notice (Section 80)

A person must comply with a requirement under a removal notice to the extent that the person is capable of doing so.

Maximum penalty: 500 penalty units.

The eSafety Commissioner may issue a formal warning if a person contravenes s80.

You can find more information online at <https://www.esafety.gov.au/image-based-abuse>.

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

Note: certain other conduct in relation to technology-facilitated stalking or abuse may constitute a criminal offence. Please see the *Legal Guide to Surveillance Legislation in WA* and the *Legal Guide on Relevant Criminal Offences in WA* for further information.

March 2022