Chapter 4: Domestic violence and technology

Advances in information and communication technology, together with increased access to such technology, have led to a rapid rise in technology-facilitated domestic violence (also known as technology-facilitated stalking and abuse). This chapter provides guidance for practitioners wanting to advise clients about technology-facilitated domestic violence.

WATCH THIS SPACE

The Commonwealth Attorney General is currently considering the introduction of law which will provide civil remedies for victims of non-consensual sharing of intimate images. so please ensure that you are up to date with any changes that may have been introduced following the writing of this chapter.

What is technology-facilitated stalking?

Technology-facilitated stalking and abuse is the use of technology, such as the internet, social media, mobile phones, computers, and surveillance devices, to stalk, harass, intimidate or humiliate a person.

Technology-assisted domestic violence has been reported to have unique impacts, some more and some less harmful than in-person behaviours. For example, victims can feel tethered to their abusive partners by technology, unable to escape.

Sharing intimate images without consent

Recent research has found that one in ten Australian adults have had a nude or semi-nude image of themselves sent to others or posted online without their consent.[20]

Sharing intimate images without consent is sometimes colloquially referred to as 'revenge porn'. This expression has been rejected as a preferred terminology because it belies diverse perpetrator tactics (not usually out of revenge) and it treats the images themselves as a form of pornography regardless of whether they would be regarded as such by ordinary community standards and may not be created for sexual gratification purposes. The term 'revenge porn' ignores the key issue – that it is abuse. 'Image based abuse' is the preferred terminology.

Image-based abuse offences

If your client has had images shared without their consent or if somebody has threatened to do so, since 25 August 2017 the *Crimes Act 1900* (NSW) has been amended to create four new Table 2 offences to address the non-consensual sharing of intimate images:

- Recording an intimate image without consent (s 91P)
- Distributing an intimate image without consent (s 91Q)
- Threatening to record an intimate image without consent (s 91R(1))
- Threatening to distribute an intimate image without consent (s 91R(2))

A summary offence of contravening an order, such as failing to take reasonable steps to take down or destroy an intimate image recorded or distributed without consent has also been created, with a maximum penalty of 50 penalty units or imprisonment for 2 years, or both. (section 91S).

Requisite mental element

For the recording and distributing offences in sections 91P and 91Q, the prosecution must prove that the act of recording or distributing is intentional, and that the person either knew that, or was reckless as to whether, the victim did not consent to the recording or distributing.

For the threat offences in section 91R, the prosecution must prove that the person who made the threat intended to cause the other person to fear that the threat would be carried out. It is irrelevant whether the image actually existed or not. These offences are particularly directed to the domestic violence context, where threats to distribute images may be used to control a person's behaviour.

Consent

Section 91O provides that a person consents to a recording or distribution of the image if the person

20 See A Powell and N Henry, 'Digital Harassment and Abuse of Adult Australians: A Summary Report', RMIT University, 2015.

'freely and voluntarily agrees' to the recording or distribution. Agreeing to the recording or distribution of an image on one occasion, or to a particular person, or in a particular way, does not mean that a person will be taken to have agreed to recording or distribution of another image, or on another occasion, or to another person, or in another way. Distributing an image of oneself does not mean that a person consents to another person distributing the same image.

People under 16 or who do not have the capacity to consent (because of, for example, cognitive incapacity) are taken not to have consented to the recording or distribution of intimate images.

Exceptions

There is an exception for the recording or distributing offences where 'a reasonable person would consider the conduct of the accused person acceptable' (s 91T). This exception is intended to ensure that the new offences do not criminalise 'socially acceptable activities'.[21]

There are no exceptions for the offences of threaten to record or distribute an intimate image.

Overlap with unlawful filming offences

There will be times when the same acts could be prosecuted under either the new recording offence in section 91P, or the existing unlawful filming (or 'upskirting' offences in section 91K and 91L of the Crimes Act 1900 (NSW)). However, the unlawful filming offences require proof that the offender had the purpose of sexual arousal or sexual gratification, while the new offence does not require proof of any particular motivation.

Offence of publishing an indecent article

It is also an offence under section 578C of the *Crimes Act 1900* (NSW) to publish an indecent article. In *Police v Ravshan USMANOV* [2011] NSWLC 40 Mr Usmanov was sentenced to six years' home detention for publishing nude photographs of his ex-girlfriend on Facebook.

Sexting, and young people as offenders and victims

The image-based abuse offences do not apply to 'sexting', that is, sending a nude picture of oneself to someone else. However, they will apply if that image is subsequently distributed without the person's consent. The approval of the NSW Director of Public Prosecutions will be required for prosecutions of children under 16 years old.

Creating, possessing or distributing sexual images of children can still be prosecuted under section 91H of the Crimes Act 1900 (NSW) and Part 10.6 of the Criminal Code Act 1995 (Cth). Section 91H concerns sexual images of a person under 16 years, and children can be prosecuted without the consent of the DPP. The Commonwealth offences concern sexual images of a person under 18 years, and the consent of the Cth Attorney-General is required to commence proceedings where a defendant is under 18 at the time of the alleged offence.

Accessing Victims Support

The three new indictable offences will also be included as "personal violence offences" in the *Crimes (Domestic and Personal Violence) Act.* This means eligibility under the NSW Victims Support scheme will be enlivened.

Working with Children Check

The working with children check (WWCC) will be triggered if an adult commits one of the offences set out below against a child. For further information on the WWCC see page 22.

Table of common behaviours and corresponding criminal offences

Perpetrators of technology-facilitated domestic violence employ many tactics. Due to perceived difficulties of evidence gathering, the impunity and anonymity technology can bring, and minimisation of the harm caused, police advocacy is often required to have matters investigated and perpetrators held to account.

In advocating for clients who have been victims of such behaviour, it can be useful to keep in mind the criminal nature of this behaviour and to push for the enforcement of existing laws. Listed below are examples of common behaviours and criminal offences that may be relevant.

See also a guide to relevant criminal offences involving domestic violence and technology at www.smartsafe.org.au/legal-guides.

21 NSW Attorney General, The Hon Mark Speakman, Second Reading Speech, 24 May 2017.

Type of behaviour	Possible criminal offences
Keeping a person under video surveillance	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Voyeurism (*Crimes Act 1900* (NSW) s 91J) ◗ Installing device to facilitate observation or filming (*Crimes Act 1900* (NSW) s 91M) ◗ Installation, use and maintenance of optical surveillance devices without consent (*Surveillance Devices Act 2007* (NSW) s 8) ◗ Possession of record of private conversation or activity (*Surveillance Devices Act 2007* (NSW) s 12) ◗ Manufacture, supply and possession of listening and other devices for unlawful use (*Surveillance Devices Act 2007* (NSW) s 13)
Listening to or recording private conversations without consent (may be facilitated by spyware apps or software)	◗ Prohibition on installation, use and maintenance of listening devices (*Surveillance Devices Act 2007* (NSW) s 7) ◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Possession of record of private conversation or activity (*Surveillance Devices Act 2007* (NSW) s 12) ◗ Manufacture, supply and possession of listening and other devices for unlawful use (*Surveillance Devices Act 2007* (NSW) s 13) ◗ Interception devices (*Criminal Code 1995* (Cth) s 474.4) ◗ Telecommunication not to be intercepted (*Telecommunications (Interception and Access) Act 1979* (Cth) s 7)
Tracking a person's location through GPS without consent	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Prohibition on installation, use and maintenance of tracking devices (*Surveillance Devices Act 2007* (NSW) s 9) ◗ Manufacture, supply and possession of listening and other devices for unlawful use (*Surveillance Devices Act 2007* (NSW) s 13)
Taking intimate images or recordings without consent	◗ Recording an intimate image without consent *(Crimes Act 1900 (NSW) s 91P)* ◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Filming a person engaged in a private act (*Crimes Act 1900* (NSW), s 91K) ◗ Filming a person's private parts (*Crimes Act 1900* (NSW) s 91L) ◗ Installation, use and maintenance of optical surveillance devices without consent (*Surveillance Devices Act 2007* (NSW) s 8) ◗ Possession of record of private conversation or activity (*Surveillance Devices Act 2007* (NSW) s 12)
Sharing intimate images or recordings without consent	◗ Distributing an intimate image without consent *(Crimes Act 1900 (NSW) s 91Q)* ◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Publishing indecent articles (*Crimes Act 1900* (NSW) s 578C) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17) ◗ Prohibition on communication or publication of private conversations or recordings of activities (*Surveillance Devices Act 2007* (NSW) s 11)

Type of behaviour	Possible criminal offences
Threatening to record an intimate image without consent	◗ Threatening to record an intimate image without consent (*Crimes Act 1900 (NSW) s 91R)*
Threatening to share intimate images or recordings without consent	◗ Threatening to distribute an intimate image without consent (*Crimes Act 1900 (NSW) s 91R(2))* ◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Documents containing threats (*Crimes Act 1900* (NSW) s 31) ◗ Using a carriage service to make a threat (*Criminal Code 1995* (Cth) s 474.150) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17)
Checking call logs, messages or accounts without permission	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Unauthorised access to or modification of restricted data held in computer (*Crimes Act 1900* (NSW) s 308H)
Making false online accounts or impersonating victims	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17) ◗ Dealing in identification information (*Criminal Code 1995* (Cth) s 372.1)
'Doxing': releasing a person's details online such as their address, phone number, email address or personal details	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17) ◗ Dealing in identification information (*Criminal Code 1995* (Cth) s 372.1)
Sending large volumes of electronic communications to threaten, intimidate or harass	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17)
Changing or demanding passwords	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Unauthorised access to or modification of restricted data held in computer (*Crimes Act 1900* (NSW) s 308H)
Making threats via electronic communications	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Documents containing threats (*Crimes Act 1900* (NSW) s 31) ◗ Using a carriage service to make a threat (*Criminal Code 1995* (Cth) s 474.15) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17)

Type of behaviour	Possible criminal offences
Blackmailing via electronic communications	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17)
Monitoring or unauthorised access of a person's social media accounts, email accounts, internet dating accounts or other accounts	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Unauthorised access to or modification of restricted data held in computer (*Crimes Act 1900* (NSW) s 308H)
Accessing a person's computer, phone or other device without their knowledge or consent	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Unauthorised access to or modification of restricted data held in computer (*Crimes Act 1900* (NSW) s 308H)
Installing spyware on electronic devices. Different spyware applications and software have varying capabilities. For example, some spyware allows you to access a person's messages, emails, photos and call logs; some allows you to intercept calls; others act as a remote listening device or tracking device, or activate an internal device camera	◗ Stalking or intimidation with intent to cause fear of physical or mental harm (*Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13) ◗ Using a carriage service to menace, harass or cause offence (*Criminal Code 1995* (Cth) s 474.17)

Evidence

There is a common misconception that it is too onerous to prove who was the person at the other end of the text, email, surveillance device or other means of electronic communication. However, in cases involving technology, there is often more evidence than an in-person matter. What is difficult is knowing how to obtain the evidence and how to have it admitted into evidence. Below are some tips about how to do this.

Email

Useful evidence can be obtained from the header of the email communication including the sender's IP address. Extracting this data is a simple process, but is different for each email service. To find out how to do this you can visit www.whatismyipaddress.com/find-headers.

Facebook

Some useful evidence may be obtained by downloading a copy of your client's Facebook data via the Facebook settings page. Facebook downloads the data into a PDF file including the IP addresses used to log in and out of Facebook, chat histories, posts, personal details, searches and photos including their metadata. Deleted content is not available and some old data may not be available if it has been deleted according to the retention schedule.

Police may also be able to obtain Facebook records if investigating a criminal matter. Investigating officers can visit www.facebook.com/records for identification information such as the user's IP address and contact details. For more formal investigations, police can use subpoenas or preservation orders from Facebook via internal mechanisms.

Google

If the client has a copy of the intimate image, they can use Google image search to see if it has been published anywhere on the internet. They can do this at images.google.com by clicking on the camera button next to the search bar and uploading their photo to see whether the image is on the internet.

If a client is concerned the image will be posted online with their personal details, they can set up a Google alert (www.google.com/alerts) to notify them of any information that is posted. For example, they could set up alerts for their name, address, email and telephone number. They will then receive email alerts with any search results that include those details.

Your client can also contact search engines such as Google to ask them to remove the content from their search results.

Phone

There are a number of apps and programs that can be used to download text messages, voicemails or online chat histories to be tendered as evidence. Alternatively, you could ask to have a device handed up and its contents produced as evidence in court.

Most deleted emails, messages, photos and documents can be recovered with the right tools.

Carriage service providers may be able to reveal information about the true source of harassing or intimidating calls or messages. Your client should contact their service provider. Carriage service providers can also be subpoenaed for records. Your clients should also be aware they have a right to complain about unwelcome or life threatening messages under the Communications Alliance *C525:2010 Handling of Life Threatening and Unwelcome Communications Industry Code*.

Many photos have metadata or EXIF data sitting behind the file, which can provide valuable evidence. This can include geotagging information (such as the longitude and latitude of where the photo was taken or uploaded) or information about the device on which it was taken. A number of websites, apps and programs allow you to scan for this information, for example www.exifdata.com.

There are many phone apps that allow clients to record incoming calls. However, clients should be warned about the provisions prohibiting the use of listening devices to record private conversations without consent and the relevant exceptions, such as protecting their lawful interest under section 7 of the *Surveillance Devices Act 2007* (NSW) (see below).

Practitioner tip

Encourage clients to screenshot evidence, including website URLs where applicable. Copies should be saved on a USB or secure cloud-based account.

Client recordings and the *Surveillance Devices Act* 2007 (NSW)

Clients may come to you with audio or video recordings taken of a domestic violence incident. While the Surveillance Devices Act prohibits the use of listening devices, s 7(3)(b) allows recording where it is reasonably necessary for the protection of a lawful interest. A recording of a domestic violence incident would likely be considered reasonably necessary for the protection of a lawful interest, being the client's safety and would be admissible evidence. In addition, section 138 of the *Evidence Act 1995* (NSW) provides grounds for the admissibility of improperly obtained evidence, taking account of its probative value and importance of the evidence to the proceedings. In our experience such evidence has been admissible.

Taking action

Report to Police

Take the screen shots of the webpage where the image has been posted, showing the image and the URL and other evidence gathered as outlined above if possible and report it to the police.

Your client can also make an online report to the Australian Cybercrime Online Reporting Network (ACORN) by visiting www.acorn.gov.au and the Office of the e-Safety Commissioner by visiting www.esafety.gov.au.

Take-down request

Your client is very likely to want to have intimate images taken down.

The Crimes Act provisions empower courts to order a person convicted of the offence of recording or distributing an intimate image to take reasonable actions to remove, delete or destroy any image recorded or distributed by the person (s 91S).

In addition, practical, informal action can be taken by contacting the website administrator, host or webmaster to request they take the image down. This can be done using the 'contact us' or 'report a problem' function or by doing a 'whois' search using whois.domaintools.com for international websites or

whois.auregistry.net.au for Australian sites. If the webmaster does not delete the picture, they may be civilly liable for the continued publication of the image. *See Trkulja v Google* (No 5) [2012] VSC 533.

In any take-down request, it is a good idea to include the following:

- sufficient information for the image or video to be identified;
- your contact details;
- your relationship to the material, for example, the pictured person, the complainant, the copyright owner, their legal representative or their support person;
- a timeframe for the image/video to be removed;
- an indication of what law (including country) is being breached, for example, copyright, defamation, criminal laws.

Your client can also contact search engines such as Google to ask them to remove the content from their search results.

WATCH THIS SPACE

The Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018 is currently before the Commonwealth Parliament. It would create a range of civil penalties for the non-consensual recording and sharing of intimate images, and give new powers to the eSafety Commissioner to compel the removal of intimate images from online locations, issue warnings and infringement notices and seek penalty orders in court.

The office of the eSafety Commissioner is currently taking reports of image-based abuse from victims. It is able to offer the following assistance:

- Referring victims to appropriate services (police, counselling, legal assistance);
- Requesting removal of the intimate image if it has been made available online (provided such a request would not interfere with police investigations);
- Keeping the victim updated on the action taken and the outcome achieved.

Despite having no powers to compel the removal of intimate images, the Office reports significant levels of compliance with its removal requests. You can find more information online at www.esafety.gov.au/image-based-abuse/action.

Copyright

Sections 32, 86, 10 and 98 of the *Copyright Act 1968* (Cth) provide that where a photo or video has been created by the victim, such as a 'selfie', the ma-

terial may be protected by copyright as the person who takes the photo is the author of that work, and the director of a film is usually the owner.

Where a couple makes the material consensually during their relationship, they may be classified as joint authors/makers who are tenants in common of copyright, presumably in equal shares. The test of joint authorship is the extent to which two or more people collaborate in the creation of a work and the amount of skill and labour each contributes. See *Cala Homes (South) Ltd v Alfred McAlpine Homes East Ltd* [1995] EWHC 7 (Ch).

Where this is the case, any publication or reproduction must be authorised by any authors/makers and a joint owner may sue for infringement without the participation of the other joint owner even if the infringer is the co-owner of the copyright. *See Prior v Sheldon* [2000] FCA 438, Wilcox J.