IMAGE-BASED ABUSE

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of September 2025.

What is image-based abuse?

Every day, billions of images are captured, uploaded online, and shared electronically. The internet facilitates rapid distribution and sharing, but it also creates an irreversible, permanent record of our actions. In Australia, image-based abuse refers to the sharing of, or the threat to share, intimate images without the consent of the person depicted in those images. Many states in Australia have enacted legislation that makes the non-consensual sharing of intimate images (NCII) a criminal offence.

In the context of domestic/family violence, abusers will often share or threaten to share intimate photos or videos of survivors to manipulate, punish, or control the survivor. Many of these videos or photos are often posted and shared online to popular social media sites or pornography or "revenge porn" websites.

When posted online, the survivor may also be 'doxxed', with some intimate images including identifying information of the individual, such as their full name, address, phone number, and place of employment or school, which can pose a significant risk of further abuse, stalking, and harassment by other perpetrators. Survivors have reported being contacted or approached by strangers asking for lewd sexual favours or more photos after their pictures or videos and personal information have been posted online.

Abusers may also send or threaten to send images directly to friends, family, and others in the community who know the victim, via email, texting, or through their DM's.

A perpetrator can come into possession of intimate photos or videos of a survivor in various ways.

- He initially took the photo or video, with or without the survivor's knowledge or consent.
- He was sent the photo or video by the person in the video (a selfie), voluntarily or by coercion.
- He stole the image by physically accessing the survivor's phone or computer or by using malware to do so.
- He photo-shopped another intimate image to make it appear as if it is an image of the survivor.
- He used 'nudify' apps or other AI technology on a survivor's videos or photos to create intimate deepfakes.

Impact on victim-survivors

The effect of this abuse can be devastating, impacting every part of the victim's life and their future. Many survivors are re-victimised in their school, workplace, or community, and some have attempted or committed suicide as a result. Unfortunately, a significant amount of victim-blaming exists in some of these cases, including suggestions that the victim should not have shared the images in the first place. Even if the images were obtained without the survivor's knowledge or consent (e.g. secretly recording someone or recording a sexual assault), the survivor's actions are often questioned. The focus of image-based abuse should not be on the survivor's actions, but on the distribution of the images without the consent of the survivor.

Terminology

Image-based abuse is often referred to as "revenge porn" or "cyber harassment." Other terms for this form of abuse include: sexploitation or sextortion, where someone blackmails another person by threatening to reveal explicit images; and e-venge, referring to the electronic distribution of images.

The current preferred term is "image-based abuse" or "non-consensual distribution of images." This terminology does not focus on the action of the survivor or the motivations of the person who shared the image (which may be motivations other than revenge). Instead, it focuses on the lack of consent by the survivor in the recording and/or distribution of the image.

Further, these images need not be sexual in nature or show nudity or genitals, which is often the criterion used to determine whether an image is considered pornographic, to be considered intimate. . The term 'intimate image' includes photos or videos that are intimate in the context of the survivor's cultural or social background.

What can survivors do?

Document what's happening

For many survivors, their first instinct is to get these images removed from the internet immediately. However, before you do that, consider whether you want to document or capture any evidence, so you have a record of what was posted and by whom. This will be important if you decide at any time in the future to report the abuse, either to the platform, the police, a lawyer, or other designated reporting bodies.

Here are some tips for documenting evidence.

- When capturing evidence digitally, ensure that the device used and the location where the evidence is stored (e.g., cloud account, app, USB drive, external hard drive etc) are secure, private, and safe.
- Capture the URL of where the image was posted.
- If the URL doesn't include it, identify the website on which it was posted.
- If the website displays the name of the person who posted the image, also capture (by taking a screenshot or screen capture) their name and any other available profile information.
- Try to capture the date and time the image was posted, and always record the date the evidence was collected.
- If there is any other related harassment, such as emails or texts, be sure to document those as well.
- If the abusive person made any statements about posting your intimate image, record that in your documentation log.

Remove the online content

You can report intimate images that have been posted online to the office of the eSafety Commissioner, which has the authority to order their removal from various online platforms and websites.

Report to the website

Many major social media websites have a process to remove non-consensual intimate images. (See eSafety's list of platforms that have formal removal processes). These companies have policies that prohibit the posting of non-consensual intimate images on their sites and, once reported, the images will be removed. It is essential to capture the evidence (e.g. post) first, before reporting it, as once it's removed, you will not have proof of where it was posted.

Some websites do not have a reporting process to take down non-consensual intimate images. If this is the case, read their community guidelines or content guidelines to see if they will remove specific content. Some websites have content guidelines that prohibit content that is harassing, abusive, hateful, or harmful. Although they don't have a take-down reporting process, they may allow content removal requests if you email or contact them directly. Some websites will remove content if there is a copyright infringement. This can be helpful if you took the photo or video.

Be cautious of websites that request a significant amount of personal information from you or require payment to remove the image. While most websites will try to be helpful, some websites may further exploit what happened to you by requesting personally identifying information so they can post it alongside the intimate image or blackmail you for more money to remove the content.

Remove your image from search engines

For some survivors, the biggest concern is that these images may appear if someone searches for them. You can use search engine removal tools, or submit a takedown request to Google or Bing and ask that they remove the URL links with your image from

search results. This way, when someone searches your name, it's not the first thing that comes up.

Hash the image

To remove "revenge porn" images, use tools like StopNCII.org and takeitdown.ncmec.org to generate a hash of your image for detection and removal by participating companies. While there's no guarantee of success, even a screenshot is worth hashing and reporting. Ensure that borders and any other content are cropped out to be as close to the original as possible. Note that AI-generated content can also be hashed!

Report the abuse

Report to police

One option is to report to the police. It is a Commonwealth offence to use a carriage service to harass, menace or offend; and depending on what state you live in, there may also be specific image-based abuse offences. To find out what general and Commonwealth laws may apply, as well as specific state-based image-based abuse legislation, visit the eSafety Commissioner's Image-Based Abuse website. You should also be aware that if the image-based abuse is part of a larger pattern of abuse, there may be other crimes that have occurred as well. Consider speaking with the police about your case and asking what they can do for you.

Report to the eSafety Commissioner

If you need assistance in reporting to the website or want more information, visit the Office of the eSafety Commissioner's Image-Based Abuse Online Portal. This online portal includes information on whom to contact to request that your intimate image be removed. You also have the option of reporting to the eSafety Commissioner's office, and they will report the image/video on your behalf. This portal also has a range of information regarding legal and support options. The eSafety Commissioner's office may even be able to investigate the image-based abuse and launch civil proceedings to hold the person who posted your image accountable.

Get legal advice

In some cases, you may want to review your civil options. This may include seeking a protection order or other civil recourse. Contact your local Community Legal Centre, Women's Legal Centre or Legal Aid Commission for advice or referral to someone who can help.

Seek support from a domestic/family violence service

If the intimate image-based abuse is part of a pattern of domestic violence, seek support from a domestic/family violence service. They can help you to deal with image-based abuse as well as the other forms of abuse you are experiencing.

Tech Safety Tips

Here are some tips that may be helpful:

- If your photos and videos are automatically uploaded to an online cloud service, verify that these accounts are secure and that no one else has access to the password. Ensure that all your online accounts are secure and that only you know the passwords associated with them.
- Review the privacy settings of your social media accounts to understand who can view the content you share. You may want to review your friends and followers, and if there is anyone you don't want to see your information, consider unfriending or removing them as a follower of your account if it is safe to do so.
- Enable passcodes, patterns, or biometric access verification on your devices, particularly those that contain photos or videos of you.
- Some devices offer hidden folders to store sensitive apps or allow you to lock individual apps for enhanced privacy and security.
- Consider creating a Google Alert for your name and social media handles to receive an alert if anything about you is posted online. This will be best for someone with a name or with social media handles that aren't very common. Also, make sure you'll be okay receiving an alert, even if that means you'll know each time your intimate image has been re-posted. Some survivors find this approach helpful, while others find it difficult.
- If you discover an intimate image of yourself online that has been posted without your consent, ensure you capture the full URL and the profile details before reporting to the platform or other reporting authorities.

Resources

The following websites may provide additional information about this issue, as well as listings for legal services and other advocacy organisations that can offer assistance.

- State-specific legal guides for technology-facilitated abuse – https://techsafety.org.au/resources/legal-guides/
- eSafety - https://www.esafety.gov.au/key-topics/image-based-abuse/report-image-based-abuse
- Stop NCII - https://stopncii.org/
- TakeItDown - https://takeitdown.ncmec.org/
- 1800 Respect – https://1800respect.org.au/