Australian Government

Australian Government response to the Senate Legal and Constitutional Affairs References Committee Report:

Phenomenon colloquially referred to as 'revenge porn'

March 2022

Introduction

The Australian Government recognises that the non-consensual sharing of intimate images is a serious and growing problem in Australia. The non-consensual sharing of intimate images covers a broad range of conduct, relationships, distribution methods and motivations, including an intention to cause harm, coerce, control, abuse, blackmail, humiliate or embarrass the subject of the material. It can have a serious impact on victim-survivors, including psychological injury or trauma, and a loss of reputation, social standing, or employment.

Non-consensual sharing of intimate images comprises one part of a broader phenomenon of technology-facilitated abuse, and can also be a form of family violence or sexual abuse. It can also constitute cyberbullying, distribution for financial gain, and in the case of minors, child abuse material.

The Australian Government appreciates the work of the Committee and those who contributed views and evidence to the Committee.

Senate Committee Report

On 12 November 2015, the Senate referred the issue of non-consensual sharing of intimate images, colloquially referred to as 'revenge porn', to the Senate Legal and Constitutional Affairs References Committee (the Committee) for inquiry and report. Terms of reference for the inquiry were:

1. the phenomenon colloquially referred to as 'revenge porn', which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm;
2. the impact this has on the targets of revenge porn, and in the Australian community more broadly;
3. potential policy responses to this emerging problem, including civil and criminal remedies;
4. the response to revenge porn taken by Parliaments in other Australian jurisdictions and comparable overseas jurisdictions; and
5. any other related matters.

The Committee held a public hearing in Sydney on 18 February 2016. The Committee received 32 public submissions and two confidential submissions from a range of stakeholders including individuals, organisations and Government departments.

The Committee's final report, Phenomenon colloquially referred to as 'revenge porn', was tabled and released on 25 February 2016. The report includes eight recommendations that the Committee considers will help address the non-consensual sharing of intimate images.

Summary of Government Response

Recommendation	Response
Recommendation 1 The committee recommends that Australian governments use the phrase 'non-consensual sharing of intimate images' or similar when referring to the phenomenon colloquially known as 'revenge porn' in legislation and formal documentation.	**Supported**
Recommendation 2 Taking into account the definitional issues discussed in this report, the committee recommends that the Commonwealth government legislate, to the extent of its constitutional power and in conjunction with state and territory legislation, offences for: • knowingly or recklessly recording an intimate image without consent; • knowingly or recklessly sharing intimate images without consent; and • threatening to take and/or share intimate images without consent, irrespective of whether or not those images exist.	**Supported in principle**
Recommendation 3 The committee recommends that the states and territories enact legislation with offences that are the same or substantially similar to those outlined in Recommendation 2, taking into account relevant offences enacted by the Commonwealth government.	**Noted**
Recommendation 4 The committee recommends that the Commonwealth government consider empowering a Commonwealth agency to issue take down notices for non-consensually shared intimate images.	**Supported**
Recommendation 5 If not already in existence, the committee recommends that the Commonwealth government establish a formal mechanism by which Commonwealth agencies and internet and social media providers regularly engage on issues relating to non-consensual sharing of intimate images.	**Supported**
Recommendation 6 The committee recommends that the Commonwealth government give further consideration to the Australian Law Reform Commission's recommendations regarding a statutory cause of action for serious invasion of privacy.	**Supported**
Recommendation 7 The committee recommends that the Commonwealth government implement a public education and awareness campaign about non-consensual sharing of intimate images for adults by empowering and resourcing the Office of the Children's eSafety Commissioner and the Australian Federal Police to build on their existing work with children in relation to cybersafety.	**Supported**
Recommendation 8 The committee recommends that all Australian police undertake at a minimum basic training in relation to non-consensual sharing of intimate images, in particular any new offences in the relevant jurisdiction.	**Supported**

Recommendations

Recommendation 1: The committee recommends that Australian governments use the phrase 'non-consensual sharing of intimate images' or similar when referring to the phenomenon colloquially known as 'revenge porn' in legislation and formal documentation.

Response:

The Australian Government **supports** this Recommendation, noting the Australian Government uses this or similar language, including 'image-based abuse'. The Australian Government recognises that the broad range of conduct and motivations related to the non-consensual sharing of intimate images is not captured by the term 'revenge porn', that use of this term can downplay the seriousness of the abuse and its impact on victim-survivors, and can imply that the subject of the material did something that justified retribution.

Recommendation 2: Taking into account the definitional issues discussed in this report, the committee recommends that the Commonwealth government legislate, to the extent of its constitutional power and in conjunction with state and territory legislation, offences for:

- **knowingly or recklessly recording an intimate image without consent;**
- **knowingly or recklessly sharing intimate images without consent; and**
- **threatening to take and/or share intimate images without consent, irrespective of whether or not those images exist.**

Response:

The Australian Government **supports this Recommendation in principle.** In 2018, the Australian Government introduced new offences for non-consensual sharing of intimate images that have strengthened the criminal penalties available for those who share or threaten to share intimate images and would apply to the conduct relevant to this recommendation.

In August 2018, the Australian Parliament passed the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (the EOSA Amendment Act). The Act prohibits the non-consensual posting of, or threatening to post, an intimate image on a 'social media service', 'relevant electronic service' (for example, email and SMS/MMS), or a 'designated internet service' (for example, websites and peer-to-peer file services). These provisions are retained in the *Online Safety Act 2021,* which came into effect in January 2022.

In addition to establishing a complaints and objections system, to be administered by the Office of the eSafety Commissioner (eSafety), the EOSA Amendment Act introduced a civil

penalty regime that gives eSafety the power to use a graduated range of responses against both perpetrators and content hosts who share intimate images without consent.

Of particular relevance to this Recommendation, the EOSA Amendment Act introduced two new aggravated offences to the *Criminal Code Act 1995* (Cth) (the Criminal Code) for the offensive use of a carriage service, where that offence involves private sexual material. The Commonwealth offence of using a carriage service to menace, harass or cause offence provides a foundation for the aggravated offences that specifically target image-based abuse. Section 474.17 has been successfully used to prosecute the non-consensual sharing of intimate images—see **Annexure A** for case citations and summaries.

The aggravated offences target the online distribution or transmission of private sexual material that occurs in a way reasonable persons would consider menacing, harassing or offensive. They will only apply to material that depicts adults (18 years and over), ensuring no overlap with existing offences for distributing child sexual abuse material (for which significantly higher penalties apply). 'Private sexual material' will capture material that depicts an adult's sexual organs or an adult engaged in a sexual pose or activity, in circumstances that give rise to an expectation of privacy.

The standard aggravated offence applies a higher maximum penalty to the offence of using a carriage service to menace, harass, or cause offence, where the commission of that offence involves the transmission, making available, publication, distribution, advertisement or promotion of private sexual material. The maximum penalty for this offence is six years' imprisonment.

Further, the special aggravated offence applies a higher maximum penalty to the offence of using a carriage service to menace, harass, or cause offence, where: a) the commission of that offence involves the transmission, making available, publication, distribution, advertisement or promotion of private sexual material, and b) before the commission of that offence, three or more civil penalty orders were made against the person under the civil prohibition and civil penalty regime introduced in the Act. The maximum penalty for this offence is seven years' imprisonment.

The aggravated offences address the intention of Recommendation 2—to specifically criminalise the non-consensual sharing of intimate images—in a way that appropriately complements the criminal justice framework and builds upon the effectiveness of existing legislation.

The aggravated offences complement the civil penalty regime introduced in the EOSA Amendment Act, applying increased criminal penalties to the most serious instances of image-based abuse to appropriately punish offenders and deter repeat offenders. Due to the constitutional limitations of Commonwealth legislative powers, the Australian Government notes that Commonwealth offences do not capture the *recording* of an intimate image without the use of a carriage service. These limitations were analysed in the Committee's report.[1] The *Online Safety (Transitional Provisions and Consequential Amendments) Act 2021* increased the maximum penalties for the standard offence of using a carriage service to menace, harass or offend from 3 years' imprisonment to 5 years' imprisonment. The *Online Safety (Transitional Provisions and Consequential Amendments) Act 2021* also increased the

[1] Pg. 29, "Phenomenon colloquially referred to as 'revenge porn'", *Legal and Constitutional Affairs References Committee*, The Senate.

maximum penalty for the standard aggravated offence where the offence involves distribution of private sexual material from 5 years' imprisonment to 6 years' imprisonment.

The Australian Government recognises the importance of having a nationally consistent criminal framework to protect victim-survivors of non-consensual sharing of intimate images. To address this, the Australian Government led the development of the *National statement of principles relating to the criminalisation of the non-consensual sharing of intimate images* (the national principles), which were agreed to by all jurisdictional ministers at the Law, Crime and Community Safety Council on 19 May 2017. The national principles provide a framework to ensure a consistent approach to the criminalisation of non-consensual sharing of intimate images.

Recommendation 3: The committee recommends that the states and territories enact legislation with offences the same or substantially similar to those outlined in Recommendation 2, taking into account relevant offences enacted by the Commonwealth government.

Response:

The Australian Government **notes** this Recommendation. The introduction of state and territory offences addressing the non-consensual sharing of intimate images is a matter for state and territory governments.

The Australian Government consulted with state and territory agencies in response to this Recommendation. States and territories advised that in addition to offences in the Criminal Code (Cth), they use the following state-based offences to prosecute the non-consensual sharing of intimate images:

- Queensland and Tasmania use broad state offences, including stalking, blackmail, indecent publishing and identity theft.
- South Australia uses *Summary Offences Act 1953* (SA) section 26C, which makes it an offence to distribute an invasive image of another person while knowing or having reason to believe that the other person does not consent to the distribution.
- Victoria uses *Summary Offences Act 1966 (Vic)* sections 41C, 41DA and 41DB, which make it an offence to intentionally distribute an image of another person contrary to community standards of acceptable conduct, or to threaten to distribute an intimate image of another person with the intention the victim believes the threat will be carried out.
- The Victorian Law Reform Commission (VLRC) is currently reviewing the justice system's response to sexual offences, including image-based offending. The VLRC has consulted with stakeholders, including victim-survivors, to identify opportunities to embed and build upon previous reforms, identify the barriers to reporting and resolving sexual offences, and make recommendations to improve the justice system's response. The Victorian Government will consider any recommendations for reform with respect to these issues.

- New South Wales uses *Crimes Act 1900* (NSW) sections 91P, 91Q and 91R, which make it an offence to intentionally record, distribute or threaten to distribute an intimate image of another person without consent.
- The Australian Capital Territory uses *Crimes Act 1900* (ACT) sections 72C, 72D and 72E, which makes it an offence for a person to distribute intimate images without consent, or to threaten to capture or distribute an intimate image of another person with the intention to cause fear that the threat will be carried out.
- The Northern Territory uses *Criminal Code Act 1983* (NT) sections 208AB and 208AC, which make it an offence to distribute intimate images without consent, or threaten to distribute intimate images with the intention to cause fear that the threat would be carried out.

Other states have progressed legislation specifically criminalising the non-consensual sharing of intimate images:

- The Western Australian Government passed the *Criminal Law Amendment (Intimate Images) Act 2019*. The Act:
  - makes it an offence to share intimate images without consent
  - empowers courts to make a rectification order requiring a person charged with the new offence to remove or destroy the image, and
  - ensures that existing offences also apply to a threat to distribute an intimate image.

- The Queensland Government passed the *Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act 2018* (the Act), commencing upon its assent on 21 February 2019. The Act amended the Criminal Code (Qld), creating offences related to the non-consensual sharing of intimate images which are consistent with Recommendation 2:
  - makes it an offence to distribute the non-consensual sharing of intimate images or prohibited visual recordings, that would also apply to sending, or threatening to send, intimate material without consent, and
  - empowers the sentencing court to make a rectification order requiring that an offender take reasonable steps to remove, retract, recover, delete or destroy an intimate image.

Recommendation 4: The committee recommends that the Commonwealth government consider empowering a Commonwealth agency to issue take down notices for non-consensually shared intimate images.

Response:

The Australian Government **supports** this Recommendation. Since 2018, the *Enhancing Online Safety Act 2015* has charged the eSafety Commissioner with this responsibility. A mechanism to quickly remove intimate images that have been posted online without consent provides immediate relief for victim-survivors. The Australian Government considers civil

avenues such as this just as important as criminal responses to address the non-consensual sharing of intimate images.

As noted in the response to Recommendation 2, in August 2018 the EOSA Amendment Act received Royal Assent. This legislation prohibits posting, or threatening to post, an intimate image of a person online without their consent, and introduces associated remedies and removal powers.

It also established a complaints and objections system administered by eSafety. Victim-survivors, or a person authorised on behalf of a victim-survivor, are able lodge a complaint directly to eSafety where there is reason to believe that a person has posted or threatened to post an intimate image without consent.

The civil penalty regime created by the EOSA Amendment Act was designed to facilitate the quick removal of images without causing additional distress to the victim-survivor. eSafety has the option to issue removal notices to perpetrators, social media service providers, relevant electronic services, and designated internet services. Removal notices require that the intimate image is removed within 48 hours after the notice has been given, or a longer period if eSafety allows.

eSafety may also take action against a person who posts, or threatens to post, intimate images online. This action includes issuing a formal warning, giving an infringement notice and seeking an injunction or civil penalty order from a court.

The range of civil remedies for the non-consensual sharing of intimate images provides more options for victim-survivors, greater discretion to the regulator, expedient and efficient resolution, and consequences for perpetrators.

These provisions have been migrated to the *Online Safety Act 2021* (OSA*)* with the timeframe for compliance with removal notices reduced from 48 to 24 hours. The definition of 'intimate image' has been broadened in the OSA to include images which 'purport to be of a person', allowing a more flexible response to cover the circumstance where an intimate image is tagged with a person's name, implying that it is an image of that person, even if it is not. This will also make clear that the creation of faked or altered images are captured by the scheme.

Recommendation 5: If not already in existence, the committee recommends that the Commonwealth government establish a formal mechanism by which Commonwealth agencies and internet and social media providers regularly engage on issues relating to non-consensual sharing of intimate images.

Response:

The Australian Government **supports** this recommendation.

The eSafety Commissioner leads and coordinates online safety efforts across Commonwealth departments, authorities and agencies. The eSafety Advisory Committee is therefore the most

appropriate vehicle for regular engagement on issues relating to non-consensual sharing of intimate images. This committee is chaired by the eSafety Commissioner and was established in 2020 to provide advice to eSafety on online safety issues relating to children.

This group meets up to four times a year and is comprised of members from relevant Australian Government Departments, academia, industry and social media providers and non-government organisations. Stakeholders have a variety of backgrounds, including in child protection, children's, online safety, education, law enforcement, Internet and social media companies.

Recommendation 6: The committee recommends that the Commonwealth government give further consideration to the Australian Law Reform Commission's recommendations regarding a statutory cause of action for serious invasions of privacy.

Response:

The Australian Government **supports** this Recommendation.

The current review of the *Privacy Act 1988*, announced as part of the Government's response to the Australian Competition and Consumer Commission's *Digital Platforms Inquiry*, is considering whether a statutory tort for serious invasions of privacy should be introduced for invasions of privacy which are not currently covered by the Privacy Act. This includes consideration of the recommendations of the Australian Law Reform Commission on this issue. The review, being conducted by the Australian Attorney-General's Department, is consulting widely on potential reform proposals and will provide a Final Report for government consideration.

Recommendation 7: The committee recommends that the Commonwealth government implement a public education and awareness campaign about non-consensual sharing of intimate images for adults by empowering and resourcing the Office of the eSafety Commissioner and the Australian Federal Police to build on their existing work with children in relation to cybersafety.

Response:

The Australian Government **supports** this Recommendation, and notes that a comprehensive range of measures, including education, awareness raising, and victim support, have been implemented.

eSafety began administering a complaints scheme for individuals experiencing image-based abuse in October 2017. Through the scheme, eSafety provides tangible support for Australians who have had their intimate images posted, or threatened to be posted, online

without their consent. eSafety helps victims regain control by providing helpful resources, reporting pathways and referrals to support services.

Downloadable guides are also available on eSafety's website for people who speak English as a second language, Aboriginal and Torres Strait Islander peoples, same sex attracted people, gender diverse people, bystanders wanting to help and people wanting to make amends for having shared intimate images without consent. There is also information on support available for victims of image-based abuse in other countries.

The website provides a step-by-step guide to making an image-based abuse report to eSafety. The image-based abuse team focus on the rapid removal of content, working with social media services, websites and search engines to facilitate the removal of reported image-based abuse material. The team liaise with police, schools and social media companies to support Australians reporting image-based abuse.

Since the scheme's commencement, eSafety has received 7,397 reports concerning over 10,000 URLs (as of 30 September 2021). eSafety has removed reported images in around 85 per cent of cases. In some cases, content was removed within a matter of hours.

In 2018 eSafety entered into a limited global pilot with Facebook to help prevent intimate images of Australians being posted and shared across Facebook, Messenger and Instagram. Since the launch, eSafety have assisted 35 victim-survivors of image-based abuse to access the pilot.

eSafety launched the eSafety Women program on 28 April 2016 as part of the Australian Government's $100 million Women's Safety Package. Under this program, eSafety has provided national face-to-face training workshops and webinars to frontline workers on technology-facilitated abuse. The aim of these workshops is to give frontline staff the skills, knowledge and tools to better assist women at risk from technology-facilitated abuse, including the non-consensual sharing of intimate images. As at 30 September 2021, 14,473 frontline workers have attended this training. In 2018, eSafety has launched a self-paced, online learning program for frontline workers, which to 30 September 2021 has supported 3,542 registered users. eSafety Women also provides web-based information and resources to raise awareness of technology-facilitated abuse and what can be done about it, including practical advice on the steps victims can take if their intimate images are shared without their consent.

The Australian Government has also provided additional funding over a number of years to support and expand these activities. As part of the 2021-22 Budget, the Government is providing $26.2 million to create a safe space online for women and children, including:

- $15.0 million over two years from 2021-22 for eSafety to bolster its investigations team into image-based abuse, adult cyber abuse, cyberbullying and harmful online content.
- $3.0 million over two years from 2021-22 for eSafety to implement technologies that identify intimate images that have been shared without consent to assist in the rapid removal of image-based abuse material.
- $3.0 million over four years from 2021-22 to address technology-facilitated abuse involving children.

- $5.2 million in 2021-22 for a new, National Online Safety Awareness campaign to raise awareness of the Government's *Online Safety Act 2021*.

The Australian Government also funded a national awareness campaign to improve community awareness of the resources available to parents to protect their children online. The Start the Chat campaign was launched on 15 March 2019 and ran until 30 June 2019 and was delivered through a range of media channels including television, radio, print, digital, out-of-home advertising and social media. While not specifically focused on the non-consensual sharing of intimate images, the campaign included a series of messages focused on the needs of vulnerable communities and aimed to enhance awareness of the online safety resources available through eSafety.

An evaluation of the campaign found that it was successful in lifting the awareness of eSafety's resources and encouraged more people to 'start the chat' – 44 per cent of parents and carers who saw the campaign indicated that they had spoken to their child as a direct result of seeing the advertising.

The Australian Government notes that these new measures will complement meaningful work that is already being undertaken by numerous government and non-government organisations (NGOs). As part of the 2019-20 Budget, the Australian Government committed $10 million to establish an Online Safety Grants Program. The Program, administered by eSafety, provides grants to NGOs over three years (2020-2023) to support online safety education and training projects.

Under round one of the Program, eSafety awarded $2.25 million across eight projects in 2020 with a further 15 projects sharing $4.5 million under Round 2 in 2021.

The Alannah Madeline Foundation, a round one grant recipient, is currently delivering the project 'Improve your play' which is delivering a range of education resources and targeted interventions to reduce technology-facilitated harm of a sexualised nature by males aged 15-17. These resources and interventions have been co-designed with a diverse group of adolescent males and females and will be released in March 2022. They are expected to have a national reach to 250 young males through forums, 10,000 people through social media and up to 10 industry platforms through advocacy.

eSafety is aware of the importance of ensuring all communities, including parents and educators, can support young people to understand the consequences of, and the avenues for reporting, the non-consensual sharing of intimate images. Twenty-five per cent of all image-based abuse reports to our investigations team are from young people under 18.

To address this issue the eSafety has developed webinar, factsheets and video content for parents and carers on the topic of 'Online sexual harassment and image-based abuse'. The webinar, launched in October 2021, includes support pathways for young people when dealing with issues of online consent, image-based abuse and pressure to share nude images. The resources explain when and how to make a report about the non-consensual sharing of intimate images to eSafety, or online sexual abuse or exploitation to the Australian Centre to Counter Child Exploitation (ACCCE) for investigation. The webinars have been attended by over 800 parents and carers to date.

eSafety has also developed educator professional learning, 'Online Harmful Sexual Behaviours, Misinformation and Emerging Technology'. The aim is to support educators to

identify, prevent and respond to harmful sexual behaviours in young people, including examples of online grooming and illustrating how coercion and pressure may be used by perpetrators. The training addresses topics including inappropriate contact, online grooming, self-produced child abuse material, image-based abuse, and sexual extortion. The training links to eSafety's extensive website resources and strategies to teach respectful relationships with a focus on identifying healthy and abusive relationships.

In addition, the Australian Federal Police ThinkUKnow program provides a national online child safety program which educates parents, carers, teachers, children and young people to help prevent online child sexual exploitation. ThinkUKnow is an evidence based, pro-technology program that addresses topics including self-produced child sexual exploitation, inappropriate contact, online grooming, image-based abuse, and sexual extortion and encourages help-seeking behaviour. The program is aligned with the Australian Curriculum and uses up-to-date research and real case studies from the ACCCE to illustrate the challenges young people may face and how to get help. ThinkUKnow is delivered nationally in partnership with State and Territory police and industry partners utilising face-to-face presentations and online resources, including parent, carer and teacher resources, fact sheets and guides.

ThinkUKnow education material provides awareness and educates young people about legal responsibilities online to prevent them from becoming offenders themselves, highlighting illegal behaviour that can lead to a young person becoming an online child sex offender.

The Australian Government also acknowledges that technology-facilitated abuse, including the non-consensual sharing of intimate images, is a tactic often used by perpetrators of domestic and family violence as a way of exerting control over and inciting fear in their partner or ex-partner. Perpetrators can also use technology to commit sexual violence, including sexual harassment, outside of a domestic setting, for example through dating apps and other online platforms. The Australian Government is addressing the growing issue of technology-facilitated abuse more broadly through the National Plan to Reduce Violence against Women and their Children 2010-2022 (the National Plan).

Under the Fourth Action Plan of the National Plan, the Australian Government committed $340 million to prevent violence before it happens and provide support to women and children. This includes $4 million to eSafety to implement the following programs:

- $2.5 million over 2019-20 to 2021-22 to work with Aboriginal and Torres Strait Islander owned and staffed support organisations to develop resources related to technology-facilitated abuse. This program is assisting Aboriginal and Torres Strait Islander women in communities across Australia to identify, report and protect themselves and their children from technology-facilitated abuse.

- $1.5 million over 2019-20 to 2021-22 to work with the disability sector to develop materials related to technology-facilitated abuse, including dedicated web and training resources, to empower frontline workers to support women with disability. These resources – including three case study videos, conversation cards and 'keep safe' cards – were launched in September 2021.

The Government is currently developing the next National Plan to End Violence against Women and Children, to commence in mid-2022. The Department of Social Services and the Office for Women are conducting public consultations to inform key priorities and focus

areas for the new National Plan. Consultation activities include the National Plan Advisory Group, the Aboriginal and Torres Strait Islander Advisory Council, virtual workshops with key participants from each state and territory, public surveys on engage.dss.gov.au, and the National Summit on Women's Safety (held on 6-7 September 2021).

Recommendation 8: The committee recommends that all Australian police undertake at a minimum basic training in relation to non-consensual sharing of intimate images, in particular any new offences in the relevant jurisdiction.

Response:

The Australian Government **supports** this Recommendation. Cybercrimes against the person (including investigations related to the non-consensual sharing of intimate images), are generally handled by state and territory police. This approach reflects the Australia New Zealand Policing Advisory Agency (ANZPAA) *Protocols for Law Enforcement Agencies on Cybercrime Investigations.*

While the introduction of training for state and territory police is a matter for state and territory governments and individual law enforcement agencies, the Australian Government considers that it is incumbent on police forces to actively support and resource such initiatives. A national approach to such training is being considered in the development of the next National Plan to End Violence against Women and Children, to commence in mid-2022.

The ANZPAA *Education and Training Guidelines for Family and Domestic Violence* were developed and approved in 2012. These guidelines are available for jurisdictional use to inform and support the development and review of education and training for police involved in incidents and/or investigations of family and domestic violence. New content on technology-facilitated abuse was recommended for inclusion in the updated curricula.

At the state and territory level, significant work is underway to educate frontline services and law enforcement officers about technology-facilitated abuse. This includes developing training modules and increased coordination of domestic violence activities across government, such as:

- risk assessment training and tools for frontline police officers to guide conversations and identify technology and social media as tools of abuse, stalking and harassment
- initiatives designed to improve the accuracy of reporting on technology-facilitated abuse
- re-aligning organisational structures to better respond to family violence matters (including technology-facilitated abuse),
- establishing specific units comprising several government agencies working collaboratively to cohesively address family violence and encourage reporting by victims of family violence.

Annexure B contains more detailed information about approaches being undertaken by states and territories.

Annexure A – case citations and summaries of relevant offences against the *Criminal Code* (Cth)

Case	Summary
R v Simonetti [2018] ACTSC 31	Simonetti sent intimate images he had discovered on 'revenge porn' websites to two teenage girls depicted in those images, threatening to distribute the images widely among their peer groups and demanding the girls send him more nude images. Simonetti was convicted of one count of using a carriage service to menace, harass or cause offence contrary s474.17 of the Criminal Code, as well as Commonwealth child abuse material offences.
R v Cartwright [2018] ACTSC 132	The teenage victim sent intimate images of herself to Cartwright before they commenced a consensual sexual relationship. Once that relationship ended, Cartwright threatened to distribute those images to the victim's new boyfriend and post them online if the victim did not send him more intimate images of her. The victim sent Cartwright more intimate images under duress. The offender was convicted of one count of using a carriage service to menace, harass or cause offence contrary to s474.17 of the Criminal Code, as well as Commonwealth child abuse material offences.
Dever v The Commissioner of Police [2017] QDC 65	When Dever lived with the victim, he found a USB in the house containing nude images and videos of sexual activity recorded by the victim privately in her bedroom. After being evicted from the house, Dever uploaded nude images and at least one video of the victim engaging in sexual activity on YouTube, without any permission to access, distribute or upload the images. Dever shared the YouTube link with the victim, another former housemate, and four other people. Dever was convicted of one count of using a carriage to menace, harass or cause offence, contrary to s474.17 of the Criminal Code, as well as counts for other offences.
CDPP v Daniel Watson [2015] VCC 1172	Watson used numerous fictitious social media accounts where he assumed different aliases to encourage teenage girls to send him photos of themselves in sexual poses. Once a girl had sent him photos he would prevail upon the girl to send more photos and videos by threatening to disclose to the girl's family and school the photos already obtained. Watson pleaded guilty to offences using a carriage to menace, harass or cause offence, contrary to s 474.17 of the Criminal Code and other Commonwealth child abuse material and grooming offences.
R v Hastings Fredrickson (No 1) [2015] NSWDC 114	During the course of a consensual sexual relationship between Fredrickson and the victim, Fredrickson set up a camera and filmed their sexual acts. The victim did not know the acts were being filmed. Fredrickson sent images taken from the filmed footage to members of a group of colleagues who called themselves the 'Jedi Council' along

	with insulting, degrading and humiliating descriptions of women. The victim did not know and did not consent to the images being emailed. Fredrickson was convicted of three counts of using carriage service to menace, harass or cause offence contrary to s 474.17 of the Criminal Code.
Grott v The Commissioner of Police [2015] QDC 142	Grott created a false online identity and struck up relationships with at least 20 underage girls and young women online. One victim sent partially nude and nude images to Grott. She told him the photographs were for him only and not to show it to any other person. Using a different online persona Grott posted a nude photograph of the victim on Instagram, and then created a new Instagram account where he posted the nude photograph and screenshots of their conversations, including abusive language. The second victim sent Grott several photographs of herself in her underwear and one nude photo. Grott sent these photographs to her Facebook friends. Grott created an online dating profile without the second victim's knowledge, in which he used photographs the second victim had sent to him, listed her phone number, and asked for sex and for people to contact her. Grott left a USB containing all the photos the second victim had sent him at that victim's uncle's workplace. The second victim attempted suicide. Grott was convicted for two counts of using a carriage service to menace, harass or cause offence contrary to s 474.17 of the Criminal Code, among other offences.
The Queen v Tamawiwy (No 4) [2015] ACTSC 371	Tamawiwy, a male impersonating a female, sent photos over Facebook of "her" exposed breasts to young men and attempted to persuade them to have sexual intercourse with "her". "She" said "she" would have sexual intercourse with each young man if he first had sexual intercourse with a male. One victim agreed to engage in sexual activity with a male in the understanding the female alias would then have sexual intercourse with him. Tamawiwy met the victim for sexual intercourse which he filmed using his phone without the victim's knowledge or consent. Tamawiwy, as his female alias, then threatened to send the video of the sexual activity to the victim's friends and workplace if he did not engage in further sexual activity with Tamawiwy. Tamawiwy did send the video and/or screenshots of the video to the victim's brother, male friend and female friend. Tamawiwy was convicted for eight counts of using a carriage service to menace, harass or cause offence contrary to s 474.17 of the Criminal Code, among other charges.
The Queen v McDonald AND Deblaquiere [2013] (unreported) –	The victim had consensual sexual intercourse with McDonald in his bedroom at the Australian Defence Force Academy (ADFA), on the condition that the relationship was confidential and neither party would tell anyone else in ADFA about it. Before the complainant arrived, McDonald initiated a connection through Skype with

litigation history at [2013] ACTSC 122	Deblaquiere on his computer. While McDonald and the complainant were engaged in sexual intercourse, their activity was being transmitted to a computer operated by Deblaquiere and was watched by him and five other cadets. The complainant was unaware of this. Both McDonald and Deblaquiere were convicted for using a carriage service to menace, harass or cause offence contrary to s 474.17 of the Criminal Code.
R v Leask [2013] WASCA 243	Leask used the internet and video chat applications to persuade five girls between the ages of 13 and 15 to remove their clothes and masturbate while video-linking or Skyping the defendant. He then threatened the victims that he would distribute footage of them engaging in sexual activity to their friends, schools and parents if they did not continue to engage in sexual activity with him via video-link and Skype. Leask was convicted for using a carriage service to menace, harass or cause offence contrary to s 474.17 of the Criminal Code.

Annexure B – relevant jurisdictional law enforcement training

Commonwealth	Australian Federal Police (AFP) investigations concerning sexual exploitation are undertaken by specialised investigators trained in managing sensitive and explicit material. Amongst the training provided is graduated exposure training, training on the triaging and safe viewing of material and legislative requirements for the collection and presentation of evidence related to this crime type. Investigators also have access to external training courses run through other government and law enforcement agencies. AFP investigators interviewing vulnerable witnesses are trained for that task. For front-line services, eSafety and WESNET jointly deliver an eSafety for Women training workshop, which receives funding support from the Department of Social Services. Additionally, Lifeline Australia's Commonwealth funded domestic violence response training program, Domestic Violence alert, is available to Australian police.
Australian Capital Territory	ACT police officers are trained to identify technology-facilitated abuse. The Crimes (Intimate Image Abuse) Amendment Bill was passed in the Australian Capital Territory in 2017, which made it a crime to share an intimate photo without consent. The Australian Capital Territory Government's Response to Family Violence (2016), identified as a priority frontline worker training, to develop a skilled and educated workforce equipped to support identification of domestic and family violence and respond effectively to the needs of victims impacted by this violence. Staff across Australian Capital Territory Government are currently expected to undertake core foundational level Domestic and Family Violence training. Staff working with targeted services which deal with domestic and family violence on a regular basis including Community and Emergency Services and Health Professionals are expected to receive higher order training. Training has been rolled out in stages, with foundational training commencing in 2019. The Domestic and Family Violence Training Strategy will build jurisdictional capacity and capability by including content in all tiers that details the different types of abuse which constitutes domestic and family violence, including the coercion and control and sexual violence commonly involved in non-consensual sharing of intimate images. ACT Policing sworn officers are not expected to complete training under the Domestic and Family Violence Training Strategy, as they already complete intensive domestic and family violence training. Members of ACT Policing's specialised sexual crimes team are also encouraged to attend cybercrime training in order to provide them with the skill to retrieve information from social media platforms.
New South Wales	The *Crimes Act 1900* was amended on 25 August 2017 to create new offences relating to the non-consensual recording or distribution of intimate images. The maximum penalty for these offences is 100 penalty units ($11,000) or imprisonment for three years. All New South Wales Police (NSW Police) officers have been informed about the new legislation. In addition, new courses and training materials have been developed to enhance the knowledge and skills of police officers to identify and investigate technology enabled crime, including non-

	consensual sharing of intimate images. Specialist training on 'technology facilitated abuse' and its use in domestic and family violence has also been developed and is delivered to officers who investigate domestic and family violence as well as Domestic Violence Liaison Officers.
Northern Territory	New offences relating to the distribution of intimate images commenced in the Northern Territory on 9 May 2018 with the legislative changes communicated across the Northern Territory Police. Awareness of cybercrime methodology and basic investigation techniques relating to technology-facilitated crimes is delivered as part of the investigator and detectives courses. Specialist courses such as child abuse and sexual assault investigations include training on the relevant legislation.
Queensland	The Queensland Police Service (QPS) deals with technology facilitated abuse during the three phases of investigative training. Content related to non-consensual sharing of intimate images also appears in a non-compulsory unit relating to child harm and sexual offence legislation and considerations. This unit is available to all QPS employees. The QPS continues to review compulsory course curriculum for front-line officers and investigators to ensure the adequacy of material available regarding the non-consensual sharing of intimate images.
South Australia	In South Australia, Part 5A—Filming and sexting offences of the *Summary Offences Act 1953* (Summary Offences Act) creates offences relevant to non-consensual sharing of intimate images. South Australia Police (SAPOL) have implemented a 'Filming and sexting offences' training package accessible through SA Police's online training environment. The course is mandatory for sworn police and unsworn staff that may be responsible for the taking of reports and/or investigation of offences under Part 5A of the Summary Offences Act. SAPOL is committed to training frontline officers and investigation specialists to continue to meet the challenges of law enforcement in a digital environment, to continue efforts to proactively raise awareness of human exploitation, and to reduce the risk of victimisation through technology facilitated abuse which includes this class of offending. In October 2018, SA Police formed the Public Protection Branch that consists of investigation and specialist units responsible for Family and Domestic Violence, Online Child Sexual Exploitation, Sexual Crime Investigations and Victim Management. The Branch also includes training officers who identify and address identified deficiencies of knowledge or policy, or changing patterns or trends in electronic facilitated abuse to inform SAPOL operations and investigations.
Tasmania	In Tasmania, the Safe Families Co-ordination Unit (SFCU) brings together staff from the Departments of Police, Fire and Emergency Management, Health, Communities Tasmania, Justice and Education working collaboratively to provide the best available information about high-risk family violence incidents. It is acknowledged that technology and social media can be used to abuse, stalk and harass in a family violence matter. Training of frontline officers remains an ongoing commitment, and training in non-consensual sharing of intimate images will be supported by initiatives such as an improved online learning environment and new

	training programs addressing scaled learning from recruit level to advanced investigator level. A Commission of Inquiry has been established in Tasmania to examine the response to sexual abuse against children. In that context, a Review Team within Tasmania Police is currently reviewing training offered to sex crime investigators and this will include any revised curriculum for basic training.
Victoria	Victoria Police has developed a Family Violence Risk Assessment Ready Reckoner for frontline police officers that was distributed to all stations in late 2015. The ready reckoner is also available for download. The ready reckoner provides questions to guide the risk assessment conversation and identification of technology and social media as tools of abuse, stalking and harassment. The ready reckoner has also been promoted through the Victoria Police Family Violence e-learning modules, published during 2016. In 2019, Victoria Police will move to the use of an actuarial tool as part of its family violence reporting to determine future risk and severity of family violence, including technology-facilitated abuse. In response to a recommendation of the Royal Commission into Family Violence, Victoria Police has opened the Centre for Family Violence, an evidence-based, holistic education centre for all ranks and across police careers. The topic of technology-facilitated family violence is included in curricula development. Victoria Police is including technology-related abuse in its updated family violence content in Foundation Training and Promotional Programs. A quick guide training film is now available on the Victoria Police Learning Hub to inform members about key issues to be alert to when investigating technology-facilitated family violence.
Western Australia	Western Australia Police (WA Police) has undergone an organisational re-structure to improve incident identification and the standard of policing response to family violence matters. WA Police is progressing a project to identify the varieties of technology that may facilitate abuse. WA Police received a grant of $375,000 from the Western Australia Government to provide protective behaviours training to the Western Australia community and police officers. This training includes online safety workshops which are provided at no cost to the participants. In addition, the WA Police provides training on technology-enabled crimes to investigators. WA Police and partners are implementing a range of education and awareness programs to ensure the smooth transition of these new laws into the community. Additional focus is being placed on key sectors, including policing and education.