



**AFPA**  
Australian Federal  
Police Association

## ***Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 [Provisions]***

Submission by the Australian Federal Police Association  
Level 3/53 Blackall Street  
Barton ACT 2600  
Tel: (02) 62851677  
Email: [afpa@afpa.org.au](mailto:afpa@afpa.org.au)

## **Introduction**

The Australian Federal Police Association (AFPA) welcomes the opportunity to make a submission to the Standing Committee on Legal and Constitutional Affairs in relation to the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*.

The AFPA thanks the Committee for this opportunity and would welcome an invitation to appear before any public hearing to provide further context or detail.

## **The AFPA**

The AFPA is a registered organisation and an autonomous sub-branch of the Police Federation of Australia. The AFPA represents the industrial, political, and professional interests of members of the AFP, law enforcement officials in the Australian Criminal Intelligence Commission, and members of the Department of Parliamentary Services.

Our members provide an essential service to Australia. They are the backbone of the Commonwealth's principal law enforcement agency, performing crucial investigative, intelligence and national security functions.

The AFP is responsible for:

- providing community policing services to the Australian Capital Territory and other territories, including Christmas Island, Cocos (Keeling) Islands, Norfolk Island and Jervis Bay,
- enforcing Commonwealth laws that combat complex, transnational, serious and organised crime, child exploitation, fraud, corruption, and cybercrime,
- protecting Australians and Australian interests from terrorism and violent extremism,
- removing wealth and property from criminals that have been illegally obtained,
- protecting Commonwealth infrastructure, including designated airports, Parliament House, and embassies,
- protecting domestic and foreign dignitaries, including the Governor-General, Prime Minister, and ambassadors,
- protecting at-risk individuals,
- representing Australian police and law enforcement at an international level and
- developing unique capabilities and exploiting advanced technology to support Australia's national interests.

## **Background**

The *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 [Provisions]* would amend the *Criminal Code Act 1995* to create offences for the transmission of sexual material without the consent of the person(s) involved. The offences would capture both unaltered material and material created and altered using artificial intelligence (AI) technology (commonly referred to as “deepfakes”).

### **What is Deepfake material?**

Realistic photos or videos of real people that have been digitally modified to depict them doing or saying things they have never actually said or done are known as “deepfakes.” They can be easily confused with authentic images or videos.

There are numerous ways in which deepfakes are utilised. They may be used, for instance, to fabricate a video in which a politician is heard saying something they did not truly say. But the great majority of deepfakes that are made and circulated are explicit.

It only takes a few minutes to make deepfakes with publicly available technology.

The capacity artificial intelligence (AI) gives criminals to create photos and videos showing actual or deepfake child sexual exploitation content represents a major source of concern for both lawmakers and police. This is especially significant in Australia. According to the CyberSecurity Cooperative Research Centre, the nation ranks third in the world for the sale of online sexual abuse material<sup>1</sup>.

### **Current difficulties facing law enforcement in Australia.**

Globally, there has been significant concern about the rise in deepfake sexually explicit material in recent years.

Under the *Online Safety Act 2021*<sup>2</sup>, certain instances of deepfake sexually explicit material being created and transmitted in Australia have resulted in legal action. Nonetheless, most people believe that the current legal framework is insufficient, both in its capacity to punish offenders and in its ability to act as a deterrent. The AFPA shares this view.

Posting private and explicit photos of someone online without that person's consent is illegal in Australia under *section 75*<sup>3</sup> of the *Online Safety Act 2021*. The maximum punishment for this civil violation is 500 penalty units<sup>4</sup> in fines. Nonetheless, the Act does not define any offences that involve taking someone's intimate photos without that person's permission.

A victim or the eSafety Commissioner may file a lawsuit under *section 75* against the distributor of deepfake sexually explicit material. The person posting the material may receive a formal warning from the eSafety Commissioner, and the social media platform, internet service provider (ISP) or other carriage service in question may receive a notice of removal. If the organisation disregards the removal notice, they risk being penalised.

This approach, however, has its drawbacks. First, civil proceedings are expensive. Secondly, there's a good chance the offender is a low-income, asset-light individual who is, therefore, effectively impervious to civil proceedings. Furthermore, it is frequently impossible to determine who distributed the images; typically, the offenders are very tech-savvy and adept at covering their tracks to avoid prosecution.

---

<sup>1</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Committees/Joint/Law\\_Enforcement/ChildExploitation47th/Inquiry\\_report/Chapter\\_2\\_-\\_The\\_crime\\_of\\_child\\_sexual\\_exploitation](https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation47th/Inquiry_report/Chapter_2_-_The_crime_of_child_sexual_exploitation)

<sup>2</sup> <https://www.legislation.gov.au/C2021A00076/latest/text>

<sup>3</sup> [https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol\\_act/osa2021154/s75.html](https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/osa2021154/s75.html)

<sup>4</sup> As of 8 July 2024, one (1) penalty unit is equal to \$313.00. Five hundred penalty units is equal to \$156,500.

There are several criminal offences that could be prosecuted in conjunction with civil proceedings for ‘creating and distributing deepfake sexually explicit material without consent.’ Using a carriage service in a menacing, harassing, or insulting manner is illegal under *section 474.17(1)* of the *Criminal Code of 1995*. The maximum sentencing provision for this offence is three years in prison or five years if it is considered an aggravated offence.

Prosecution of those who share deepfake pornography is becoming exceedingly challenging for several reasons.

Police must first determine who the victim is (and whether they are actually a real person). The AFP-led Australian Centre to Counter Child Exploitation (ACCCE) is a world-leading investigator of child exploitation. An important function of the ACCCE is locating vulnerable children who are being exploited and removing them to safety while prosecuting or assisting in the prosecution of the offenders.

ACCCE investigators spend countless hours trying to locate victims; this takes up valuable time and limited resources, as well as necessitating investigation across countries and police jurisdictions. With the creation of deepfake child exploitation material increasing, the role of law enforcement and identifying a victim is becoming exponentially more difficult. How long do investigators spend trying to find a child who potentially doesn't even exist or who had their likeness stolen but has ultimately not been abused themselves?

Deepfake sexually explicit material is becoming so realistic and sophisticated that it is increasingly difficult for a human to determine if an image is real or fake. As AI technology continues to develop at a rapid pace, eventually, only AI technology itself will be able to determine if material is real or a fake.

Another concern is locating the original location of a deepfake offence (where the material was originally created). Although deepfake sexually explicit material contains metadata that connects them to an internet protocol address, this can be readily gotten around by using a virtual private network (VPN), making it hard to identify the person who created the material or even the originating location and jurisdiction.

Many people who fall prey to deepfake sexually explicit material are unaware of who the creator is and are unable to provide proof of the source of the photographs. Moreover, the offender is also not governed by Australian laws if they committed the offence outside of Australia.

Because no physical injury has occurred to the victim, many are reluctant to disclose the abuse due to embarrassment or because they believe the incident is not serious enough to justify an investigation. This mindset needs to change, and victims must be encouraged to come forward and report instances of deepfake crimes.

The AFPA believes that a dedicated education campaign introducing the new laws would benefit the Australian community, specifically by raising awareness of this crime type in relation to the rapid advances in AI technology.

The AFPA would also support an online reporting mechanism where people can upload images and videos of deepfakes for review and potential investigation by a law enforcement agency. The AFPA acknowledges that online reporting of ‘image-based abuse’ is already available via the eSafety Commissioner’s website, however, believes the current model needs to be overhauled – involving direct referral of the crime(s) to a law enforcement agency.

The lead law enforcement agency, such as the AFP-led ACCCE, could conduct a preliminary review and, if an offence was determined to have occurred, refer the matter to the relevant state and territory police jurisdiction for further investigation. Alternately, the ACCCE could decide to conduct the operation and investigation themselves, utilising the expertise of the AFP and its workforce. If the review is referred to a state or territory law enforcement agency it is envisaged that the ACCCE would continue to support the state or territory law enforcement agency, especially if it was identified that the offender resided overseas.

The AFPA believes that online reporting would also benefit victims, by making people more likely to report deepfake sexually explicit material. From a victim's perspective, it is frequently difficult and traumatic to walk into a police station and present sexually explicit images portraying oneself in artificial scenarios. Online reporting would allow victims the opportunity to report from an environment that they are comfortable in, surrounded by support people if they choose.

### ***Case study of limitation in current legislation***

The eSafety Commissioner filed a lawsuit against Mr Antonio Rodondo in 2023 for posting deepfake pornographic pictures of multiple women on his website.

After reviewing the situation, the eSafety Commissioner issued Mr Rodondo with a notice of dismissal, forcing him to remove the material from the site and delete all intimate images of the victims.

Mr Rodondo, who lives in the Philippines, did not delete the pictures, and he later travelled to Queensland. Due to his violations of the *Online Safety Act*, the eSafety Commissioner filed a Federal Court of Australia lawsuit against him. Mr Rodondo was given an order by the court to take down the pictures from his website and to stop sharing or transmitting any further private photos.

When Mr Rodondo disobeyed the orders, he was accused of three counts of contempt of court and fined \$15,000. It is important to note that the proceedings instituted by the eSafety Commissioner were civil, not criminal.

Due to limited resources and a lack of dedicated and direct relevant legislation relating to deepfake sexually explicit material, investigators were forced to 'cobble' together offences to prosecute. Six further charges relating to 'obscene publications and shows' were brought against Mr Rodondo.

### ***Review of the Criminal Code Amendment (Deepfake Sexual Material) Bill 2004.***

The AFPA has reviewed the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2004* and fully supports it in its entirety.

### ***Recommendations***

- 1. The development of a dedicated and targeted campaign to educate the Australian community on the rise of deepfake and AI technology.**
- 2. The creation of an online reporting portal to enable victims to refer deepfake images and videos for preliminary review by law enforcement agencies to determine whether a criminal offence has occurred.**

### ***Conclusion***

The AFPA thanks the Standing Committee on Legal and Constitutional Affairs for this consultation opportunity.

In response to the harm caused by deepfakes and other artificially generated sexual material on the internet, the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024* will increase already-existing Commonwealth criminal offences and introduce new ones. The AFPA believe the Bill should be supported.