**9a Deepfakes - Non-consensual pornographic material**

**Overview**

A deepfake is a technique of image manipulation where artificial intelligence and deep learning is leveraged to utilise and manipulate a person's characteristics, including a person’s physical appearance and voice, to create an image or video that looks real. While fake and edited videos are nothing new, this recent phenomenon has caused concern due to the ease and accessibility of their creation.

The concerns surrounding deepfakes stem from their ability to be used for all sorts of unethical reasons, such as the recent creation and spread of non-consensual pornographic material in Australia.

In Australia, there is currently no single piece of legislation that deals with the creation and use of deepfake technology. However, there are several laws that may apply to deepfakes depending on the circumstances in which they are created or used. These include the:

* *Criminal Code Act 1995* (Cth);
* *Telecommunications Act 1997* (Cth);
* *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth); and
* *Online Safety Act 2021* (Cth).

Most Australian jurisdictions have criminal offences that cover the non-consensual sharing or distribution of intimate or explicit images (some of which may apply to altered material). For instance, in NSW, creating and spreading deepfake pornography is unlawful under section 474.17 and 474.17A of the *Criminal Code Act 1995* (NSW). Victoria is the only jurisdiction that has expressly criminalised both the production and distribution of deepfakes (section 53 of the *Crimes Act 1958* (Vic)).

The *Online Safety Act 2021* (Cth) provides the eSafety Commissioner (**Commissioner**) capacity to provide a removal notice to online providers (e.g. Meta) which host intimate imagery, requiring them to remove the image within as short of a time period as 24 hours, and penalise those who fail to do so. This is an essential step to preventing harm, as ‘detection without removal offers little solace to those exploited by deepfake pornography’.[[1]](#footnote-1)

The Commissioner’s powers are, arguably, insufficient to deal with all deepfake pornographic material. This is highlighted by the recent case of *Anthony Rondondo v eSafety Commissioner* (2023). Rondondo was provided a removal notice by the Commissioner to remove explicit, non-consensual pornographic material off his website, however this request was ignored, and the matter eventually went to court. Rondondo was ordered to pay $25,000 for contempt of court (failing to remove the images) plus the Commissioner’s costs.[[2]](#footnote-2)

Whilst civil penalties can be a deterrent, the Commissioner has limited criminal jurisdiction. Only a month after his civil conviction, Rondondo was arrested for distributing deepfake images of students and teachers at a Brisbane school.

**Criminal Code Amendment (Deepfake Sexual Material) Bill 2024**

In 2024, the Australian Parliament passed the *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024* (‘**Deepfake Bill’**)**.** The Deepfake Bill marks a significant step forward in Australia’s efforts to address the harms caused by deepfake materials, with a particular focus on the creation and distribution of sexually explicit material without consent. The amendments included in the Deepfake Bill would:

* Make it illegal to create deepfake sexually explicit content of a person without their consent.
* Introduced two aggravated offences to include an increased penalty for people found to have not only distributed the material in question, but were found to have contributed to the creation of the sexually explicit material and the aggravated offence of being a repeat offender.
* Imposes a maximum penalty of 6 years’ imprisonment for those transmitting the sexually explicit material without consent, with the aggravated offences each carrying a maximum penalty of 7 years’ imprisonment.

Opposition

The introduction of the Deepfake Bill has not been without opposition. It has been argued that the new provisions are already covered in other legislation, and that the new provisions encroach on the freedom of expression.[[3]](#footnote-3)

**International jurisdictions**

Internationally, several jurisdictions have taken steps to address the issue of deepfake sexual material.

United Kingdom

In April 2024, the UK government announced plans to amend the *Criminal Justice Bill* to include a new offence for making sexually explicit deepfakes without consent, which will build on section 66B of the *Sexual Offences Act 2003* (UK).

United States

The US was one of the first jurisdictions to address the regulation of deepfake legislation, however this primarily occurs at the state level. Several states have introduced laws to address specific applications of deepfake technology. California and Texas were among the first states to introduce laws specific to deepfakes in 2019.

In California, two laws were passed that focus on specific applications of deepfake technology: [Assembly Bill 602](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602) (‘**AB 602**’) and [Assembly Bill 730](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730) (‘**AB 730**’). AB 602 targets and establishes sanctions for individuals and companies that create and distribute non-consensual pornographic deepfake material, as well as provides remedies in the form of compensation and redress for victims. On the other hand, AB 730 focuses on deepfakes that can influence political campaigns, prohibiting the distribution of any manipulated content within 60 days of an election. It also allows for injunctive or equitable relief and damages to be sought by the candidate targeted by the deepfake.

Similar to California, in 2019, Texas passed a law that prevents the distribution of political deepfakes within 30 days of an election. Other states, like Virginia and New York, have since passed similar laws to address the misuse of deepfakes, specifically in criminalising the publication of sexually explicit deepfakes of an individual.

At the federal level, no comprehensive federal law has been enacted. However various federal Bills are currently under consideration by Congress that focus on regulating the creation and disclosure of deepfakes, particularly the dissemination of election-interfering deepfakes and non-consensual pornography. The proposed bills are currently under review and aim to form a more coordinated national approach to the creation, disclosure and dissemination of deepfakes in the US. For example:

* The [DEEP FAKES Accountability Act](https://www.congress.gov/bill/118th-congress/house-bill/5586/text) focuses on providing legal recourse to victims of harmful deepfakes and protecting national security against the threats posed by deepfake technology. A task force within the Department of Homeland Security would also be established to analyse and mitigate the dangers caused by deepfakes, as well as promote increased funding and research into their detection.
* The [DEFIANCE Act of 2024](https://www.congress.gov/bill/118th-congress/house-bill/7569/text) seeks to enhance the legal recourse for victims of non-consensual digital forgeries. This Act allows victims of sexually explicit deepfakes to pursue civil remedies against those who produced the images. The introduction of this Act was initially prompted by the sexually explicit AI-created images of Taylor Swift that emerged at the beginning of 2024. These proposals reflect the growing recognition of the need for federal oversight in the US.

European Union

In the European Union, the [EU Directive on combating violence against women and domestic violence](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401385&qid=1716884102079) is a directive adopted in May 2024 which requires member states to criminalise the non-consensual production, manipulation, or altering of material that makes it appear as though a person is engaged in sexual activities, including through the use of artificial intelligence.

China

The Chinese government first introduced laws relating to deepfakes in 2019, known as the ‘Regulations on the Administration of Networked Audiovisual Information Services’. This law requires individuals and organisations to disclose when deepfake technology is utilised in any videos or media, and prohibits the distribution of deepfake content that is not clearly labelled by a disclaimer.[[4]](#footnote-4) These regulations formed new rules and responsibilities for both users and providers of “audio and video information services” to monitor and control any deepfake content, including through implementing deepfake detection technology, conducting security assessments, preventing circulation of such content and reporting illegal deepfakes. Whilst service providers are responsible for the management of content on their platforms, these regulations also make it possible for users of deepfake creating services to be liable for prosecution.

Building on the 2019 regulations, new provisions were established in 2023 by the Cyberspace Administration of China (**‘CAC’**), known as the ‘Regulations on Deep Synthesis Management of Internet Information Service’ which further increased China’s control over deepfake technology throughout its lifecycle, from creation to distribution. These new provisions echo many of the requirements of the 2019 regulations, such as the heavy focus on the role of service providers, the tagging of deepfakes, the possibility of criminal prosecution and the focus on social morality. These provisions also aim to strengthen the need for training data management, as well as incorporate a requirement for platforms to remind users that they must notify and obtain consent before using the facial and vocal likeliness of other people in deepfakes.

1. Tong, S, “You Won'T Believe What She Does!': an Examination into the Use of Pornographic Deepfakes

   as a Method of Sexual Abuse and the Legal Protections Available to its Victims" [2022] *UNSWLawJlStuS*

   *25; UNSWLJ Student Series* No 22-25. [↑](#footnote-ref-1)
2. See Laura Lavelle, ‘Antonio Rotondo guilty of contempt of court after allegedly creating deepfake images of school students and teachers’ (ABC News) (6 December 2023) <<https://www.abc.net.au/news/2023-12-06/qld-deepfake-images-court-charge-antonio-rotondo-school-students/103195578>> [↑](#footnote-ref-2)
3. Billi Fitzsimmons, ‘A Victorian teen has been arrested after fake nudes of 50 school girls were shared online’ *The Daily Aus* (online, 13 June 2024) < https://www.newsletter.thedailyaus.com.au/p/teen-arrested-fake-ai-images>. [↑](#footnote-ref-3)
4. Cyberspace Administration of China, Regulations on the Administration of Networked Audiovisual Information Services (18 November 2019) http://www.cac.gov.cn/2019-11/29/c\_1576561820967678.htm [perma.cc/E2DQ-ZHCQ]. [↑](#footnote-ref-4)