Parliament of New South Wales
Parliamentary Research Service

RESEARCH PAPER: 2025-02

Sexually explicit deepfakes and the criminal law in NSW

Tom Gotsis BA, LLB, Dip Ed, Grad Dip Soc Sci
Research Analyst

April 2025

Key points

- Deepfakes are highly realistic but false images, video, audio or text. They were developed in 2017 and have since proliferated. In 2023, sexually explicit deepfake videos accounted for 98% of the 95,820 deepfake videos that were online. Most of the victims depicted in sexually explicit deepfakes are women.
- Sexually explicit deepfakes are associated with emotional, personal and societal harms, and have been viewed as a form of image-based sexual abuse and AI-facilitated abuse.
- In 2022, Victoria introduced offences that prohibit producing, distributing or threatening to distribute intimate images of adults. The definition of intimate images covers sexually explicit deepfakes.
- In 2024 Commonwealth offences were introduced to prohibit a person from using a carriage service, such as the internet, to transmit sexually explicit deepfakes of adults.
- NSW does not have offences that expressly prohibit the production and distribution of sexually explicit deepfakes of adults. The most relevant offences were introduced in 2017 and prohibit the recording and distribution of intimate images.
- Consequently, it is doubtful whether the production of sexually explicit deepfakes of adults is prohibited in NSW. The in-person distribution of sexually explicit deepfakes, and threats to do so, may also not be prohibited in NSW, depending on whether a particular deepfake was altered or generated anew.
- The limitations and uncertainties relating to NSW's intimate image offences could be remedied if they were amended along the lines of the new Commonwealth and Victorian offences.

Contents

1. Introduction

The term 'deepfakes' refers to highly realistic but fake digital material that has been created using artificial intelligence and which depicts a real person doing or saying something which they did not do or say. While there is a variety of uses for deepfake technology (including in the fields of art and cinema), sexually explicit deepfakes, or deepfake pornography, accounted for 98% of the 95,820 deepfake videos that were online in 2023.[1] The 2023 data indicated that 99% of the persons depicted in sexually explicit deepfakes were women.[2]

The most well-known cases of sexually explicit deepfakes have involved celebrities, such as the popstar Taylor Swift.[3] However, the proliferation of deepfake technology since its development in 2017 has meant that anyone can now be a perpetrator or a victim. For instance, in January 2025, a male high school student in NSW was referred to police for allegedly creating and distributing sexually explicit deepfake images of female students.[4] This followed a similar incident in a Victorian school in June 2024, where sexually explicit deepfake images of 50 female students were created and distributed online without consent.[5] In April 2025 it was reported that at least 16 public servants in Canberra were victims of more than 100 sexually explicit deepfakes created by a 23 year old man.[6]

The potential harms of sexually explicit deepfakes have been discussed in the literature and include emotional, personal and societal harms. Concerns have also been raised that deepfake technology poses particular risks to intimate partners.[7] The NSW Legislative Council is currently conducting an inquiry into the 'impacts of harmful pornography on mental, emotional and physical harm'; with the terms of reference for the inquiry expressly including 'deepfake or AI-generated pornography'.[8]

The primary purpose of this paper is to examine the Commonwealth and NSW criminal laws relating to sexually explicit deepfakes of adults. Those criminal laws are the Commonwealth offences that were introduced by the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* (Cth) and the NSW offences that were introduced by the *Crimes Amendment (Intimate Images) Act 2017*.

---

[1] H Ajder, G Patrini, F Cavalli & L Cullen, *The State of Deepfakes: Landscape, Threats and Impact*, Deeptrace, September 2019, p 1 and Security Hero, *2023 State of deepfakes: Realities, Threats and Impact*, n.d., accessed 17 February 2025. See also: J Grant, *Addressing deepfake image-based abuse*, eSafety Commissioner, 24 July 2024, accessed 17 February 2025. Note that some academics have suggested data on the prevalence and content of deepfakes should be viewed cautiously, as this is an emerging area of research: A Birrer and N Just, What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape, *New Media and Society*, 2024.

[2] Security Hero, *2023 State of deepfakes: Realities, Threats and Impact*, n.d., accessed 17 February 2025.

[3] E Saner, Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box', *The Guardian*, 31 January 2024. 94% of the persons depicted in sexually explicit deepfakes worked in the entertainment industry: Security Hero, *2023 State of deepfakes: Realities, Threats and Impact*, n.d., accessed 17 February 2025.

[4] E Rix, Sydney high school senior investigated by police over deepfake pornographic images of female students, *ABC News*, 9 January 2025.

[5] R Whitson, Principals say parents need to be vigilant as explicit AI deepfakes become more easily accessible to students, *ABC News*, 25 June 2024

[6] S Giuliani, Public servants targeted in 'sickening' deepfake scandal, *Herald Sun*, 28 April 2025.

[7] K Lucas, Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology, *Victims and Offenders*, 2022, Vol 17 p 647-659.

[8] NSW Parliament, Legislative Council, Standing Committee on Social Issues, *Inquiry into the impacts of harmful pornography on mental, emotional and physical harm*, Terms of Reference, 6 August 2024.

The paper identifies 3 gaps in NSW's intimate image offences in relation to sexually explicit deepfakes of adults. Firstly, the non-consensual production of sexually explicit deepfakes of adults for personal gratification is unprohibited in NSW. Secondly, NSW's intimate image offences may not prohibit the use of sexually explicit deepfakes to threaten, blackmail or extort someone in person. Thirdly, NSW's intimate image offences may not prohibit one person showing a sexually explicit deepfake to another person. The second and third gaps arise if the sexually explicit deepfake was created by generating a completely new image, rather than by altering an existing image. These 3 gaps are not covered by the Commonwealth's deepfake offences, as the Commonwealth offences apply only when a carriage service, such as the internet, has been used to transmit sexually explicit material.

The paper also examines the counterpart legislative provisions in Victoria, whose terms cover the gaps identified in the NSW provisions with respect to sexually explicit deepfake images and videos of adults. Recent developments in South Australia and the United Kingdom to introduce offences that cover sexually explicit deepfakes of adults are also noted.

The Commonwealth and NSW offences prohibiting child abuse material are also examined. The broad terms in which those offences are cast suggests that they prohibit deepfake child abuse material.

2. Deepfakes

2.1 Definition

A 2024 systematic literature review found that there is as yet no universally accepted definition of the term deepfake.[9] Table 1 sets out definitions that have been used by government, industry and academia. In line with the findings of the 2024 review, these definitions are cast in broad terms. In particular, they do not specify the various AI technologies that can be used to create deepfakes, such as generative adversarial networks (GANs) and autoencoders.[10] Nor do they consistently refer to the types of deepfake material that can be created, such as video, images, audio and text.

The definitions in Table 1 suggest that the use of artificial intelligence (AI) technology to generate false but convincingly realistic material is the core feature of a deepfake. This core feature distinguishes deepfakes from so-called 'cheap fakes' or 'shallow fakes'. Having been created by means other than AI (such as the use of graphic design software to copy the face of one person and paste it on the body of another person), 'cheap fakes' are generally less realistic than deepfakes and relatively easier to spot as being fake.[11]

[9] A Birrer and N Just, What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape, *New Media and Society*, 2024.

[10] 'An autoencoder is an artificial neural network trained to reconstruct input from a simpler representation. A GAN is made up of 2 competing artificial neural networks, one trying to produce a fake, the other trying to detect it. This competition continues over many cycles, resulting in a more plausible rendering of, for example, faces in video': United States Government Accountability Office, *Science and Tech Spotlight: Deepfakes*, February 2020. For a technical discussion of how deepfakes are made, see: C Bernaciak and D Ross, *How easy is it to make and detect a deepfake?*, Carnegie Mellon University Software Engineering Institute, 14 March 2022.

[11] F Celli, Deepfakes are coming: Does Australia Come Prepared? *Canberra Law Review*, 2020, 17(2), p 194-195.

Table 1: Deepfake definitions

Source	Definition
eSafety Commissioner	'A deepfake is a digital photo, video or sound file of a real person that has been edited to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say. Deepfakes are created using artificial intelligence software that currently draws on a large number of photos or recordings of the person to model and create content.'[12]
Australian Parliament	Deepfakes are '… images, videos or sound files, generated using AI, of a real person that has been edited to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say'.[13]
Commonwealth Scientific and Industrial Research Organisation (CSIRO)	'Deepfakes are synthetic media generated using artificial intelligence (AI), including images, videos, audio and even text. Most commonly, deepfakes are videos or images of people that have been digitally manipulated by cyber attackers to mislead. Deepfakes can depict people saying or doing something they never actually did.'[14]
United States Government Accountability Office	'A deepfake is a video, photo, or audio recording that seems real but has been manipulated with AI. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech. Deepfakes can depict someone appearing to say or do something that they in fact never said or did.'[15]
The Alan Turing Institute	'AI-generated video, image or piece of audio content that is designed to mimic a real-life person or scene. The content might be created from scratch, or pre-existing content may have been manipulated.'[16]
European Parliament	'… deepfakes are defined as manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning'.[17]

It is not surprising that there is as yet no universally accepted definition of the term deepfake, given that AI technology is relatively new and rapidly evolving. But it is significant for the purpose of defining deepfakes in criminal offences, as it calls for the use of broad definitions that can accommodate the rapid technological developments that characterise the field of AI.

2.2 Development

Deepfake technology was first discussed in a 2016 conference paper that described the use of 'face capture and tracking algorithms' to transfer the facial expressions of one person over the facial

[12] eSafety Commissioner, *Deepfake trends and challenges: position statement*, 23 January 2022, accessed 18 February 2025.
[13] Criminal Code Amendment (Deepfake Sexual Material) Bill 2024, Explanatory Memorandum, p 3.
[14] M Clarke, Keeping it real: How to spot a deepfake, CSIRO, 9 February 2024, accessed 28 April 2025.
[15] United States Government Accountability Office, *Science and Tech Spotlight: Deepfakes*, February 2020.
[16] P Swatton and M Leblanc, *What are deepfakes and how can we detect them?,* The Alan Turing Institute, 7 June 2024, accessed 18 February 2025.
[17] M Van Hurst, P van Boheem, D Das et al, *Tackling deepfakes in European policy*, July 2021, European Parliament, Study Panel for the Future of Science and Technology, p 2.

expression of another person.[18] In 2017, sexually explicit videos that falsely appeared to feature celebrities were posted on the social media forum Reddit. The sexually explicit videos were posted by a Reddit user with the alias 'deepfakes', who had created the sexually explicit videos using open-source AI software to adapt the techniques discussed in the 2016 conference paper.[19]

The use of open-source AI software is a significant consideration, as it has made the process of producing deepfakes more accessible and less complex; which, in turn, has led to an increase in the number of deepfakes being produced:

> These deepfakes were, and still are, generated using open-source AI technology. This means that the technology is available for the public to 'run, copy, distribute, study, change, share and improve for any purpose' on a wide scale. Accordingly, the methodology to create deepfakes has drastically improved, making deepfake creation much more widely accessible. While the creation of deepfakes would initially take weeks or months, it now only takes minutes or hours, and is only a five-step process requiring no more than a computer and two high quality videos of the subject whose face is being transposed. The software is often free and available on computers or smartphones. This ease of creation has led to an exponential increase in the number of pornographic deepfakes, with numbers online doubling every six months since their first appearance in 2017.[20]

One report found that in 2023 there were 42 'user friendly tools making deepfake content generation more accessible than ever'; with 40% being downloadable applications and 60% being web-based applications.[21] The report added that one in every 3 deepfake tools allow users to create sexually explicit deepfakes and that 'it now takes less than 25 minutes and costs $0 to create a 60-second deepfake pornographic video of anyone using just one clear face image.'[22]

2.3 Prevalence

There is no single authoritative source of data on the prevalence of sexually explicit deepfakes; with some academics noting that the existing data should be viewed cautiously, as this is an emerging area of research.[23] There is, however, a body of stakeholders and academics who view the available data as establishing that there has been a prolific increase in the number of sexually explicit

---

[18] F Celli, Deepfakes are coming: Does Australia come prepared?, *Canberra Law Review*, (2020) 17(2) 193 at 194, referring to a conference demonstration that was published as: J Thies et al, Demo of Face2Face: Real-time Face Capture and Reenactment of RGB Videos', *Proc. Computer Vision and Pattern Recognition*, July 2016.

[19] F Celli, Deepfakes are coming: Does Australia come prepared?, *Canberra Law Review*, (2020) 17(2) 193 at 194.

[20] S Tong, '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] *UNSW LawJl Stus* 25 (footnotes omitted). A similar point is made by: A Flynn, J Clough and T Cooke, 'Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse', Chapter 29, p 584-585, in A Powell et al (eds), *The Palgrave Handbook of Gendered Violence and Technology*, 2021.

[21] Security Hero, *2023 State Of Deepfakes: Realities, Threats, and Impact*, n.d., accessed 25 February 2025. The collection of the data in the Security Hero report covers the period 15 July 2023 to 29 August 2023.

[22] Security Hero, *2023 State Of Deepfakes: Realities, Threats, and Impact*, n.d., accessed 25 February 2025.

[23] A Birrer and N Just, What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape, *New Media and Society*, 2024.

deepfakes and that women are the subject of most sexually explicit deepfakes.[24] Concerns have also been raised that deepfake technology poses particular risks to intimate partners.[25]

eSafety Commissioner Julie Inman Grant has stated:

> There is compelling and concerning data that explicit deepfakes have increased on the internet as much as 550% year on year since 2019. It's a bit shocking to note that pornographic videos make up 98% of the deepfake material currently online and 99% of that imagery is of women and girls.[26]

The latest data located was for 2023 and is set out in Table 2.[27] The data relates to deepfake videos and does not include deepfake images, audio or text.

Table 2: Prevalence of deepfake videos (2023)

Indicator	Number / percentage
Deepfake videos online	95,820
Increase in the number of deepfake videos online since 2019	550%
Deepfake videos online that are sexually explicit	98%
Persons depicted in sexually explicit deepfake videos who are women	99%
Persons depicted in sexually explicit deepfakes who work in the entertainment industry	94%

Source: Security Hero

2.4 Harms

2.4.1 Adults

Sexually explicit deepfakes are often referred to as a form of image-based sexual abuse (IBSA). IBSA refers to the non-consensual creation and/or distribution of sexually explicit images of a victim that are real or which have been altered. Sexually explicit deepfakes can also be conceived of as a form of AI-facilitated abuse (AIFA).[28] AIFA encompasses all AI output (videos, images, audio and text) and

[24] The latest available data is provided in a report by the cybersecurity company Security Hero, in its report *2023 State Of Deepfakes: Realities, Threats, And Impact*, n.d., accessed 25 February 2025. The collection of the data in the Security Hero report covered the period 15 July 2023 to 29 August 2023. For earlier data that was broadly in line with the 2023 data, see: H Ajder, G Patrini, F Cavalli & L Cullen, *The State of Deepfakes: Landscape, Threats and Impact*, Deeptrace, September 2019. For examples of academic articles commenting on the increasing prevalence of deepfakes and sexually explicit deepfakes, see: F Celli, Deepfakes are coming: Does Australia Come Prepared? *Canberra Law Review*, 2020, 17(2), p 194; and S Tong, '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] *UNSW LawJl Stus* 25.

[25] K Lucas, Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology, *Victims and Offenders*, 2022, Vol 17 p 647-659.

[26] J Grant, *Addressing deepfake image-based abuse*, eSafety Commission, 24 July 2024, accessed 25 February 2025.

[27] Security Hero, *2023 State Of Deepfakes: Realities, Threats, And Impact*, n.d., accessed 25 February 2025. The collection of the data in the Security Hero report covers the period 15 July 2023 to 29 August 2023.

[28] The term 'AI-facilitated abuse' is used in: A Flynn, J Clough and T Cooke, 'Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse', Chapter 29, p 585, in A Powell et al (eds), *The Palgrave Handbook of Gendered Violence and Technology*, 2021.

acknowledges the possibility that future research may identify unique harms associated with the appropriation and exploitation of a person's identity by AI.

While there is little empirical research on the specific harms arising from AIFA compared with the more extensive body of research on the harms arising from IBSA,[29] many of the harms identified in studies examining IBSA are 'highly applicable' to deepfake victimisation.[30] The harms which have been identified include high levels of emotional harm (distress, humiliation, fear and intimidation); an inability to work, concentrate or eat; a continuous state of hypervigilance; use of alcohol or drugs to cope with emotional harm; social withdrawal; diminished career prospects; and damage to professional, personal and social relationships. Victims must also cope with the realisation that images may be viewed online millions of times and that it can be difficult to remove their online presence.[31]

Harms to a victim's privacy and autonomy that can occur when they are depicted in sexually explicit deepfakes that are created solely for personal gratification have also been discussed:

> The mere act of creating deepfakes violates the sexual privacy of the victims via a 'thievery of autonomy', as they are essentially 'a form of virtual sexual coercion and abuse that allows people to virtually undress and take advantage of women they know'.[32]

The victim's core expectation that sexual activity should be founded on consent is also violated.[33]

This harm arises even where a sexually explicit deepfake is not distributed because:

> … being able to reveal one's naked body ... at the pace and in the way of one's choosing is crucial to identity formation. When the revelation of people's sexuality or gender is out of their hands at pivotal moments, it can shatter their sense of self.[34]

---

[29] A Flynn, A Powell, A Scott and E Cama, Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse, *The British Journal of Criminology*, 2022, 62 1341-1358 at p 1343. A Flynn, J Clough and T Cooke, 'Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse', Chapter 29, p 587, in A Powell et al (eds), *The Palgrave Handbook of Gendered Violence and Technology*, 2021 and S Tong, '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.

[30] A Flynn, J Clough and T Cooke, 'Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse', Chapter 29, p 587, in A Powell et al (eds), *The Palgrave Handbook of Gendered Violence and Technology*, 2021.

[31] A Flynn, J Clough and T Cooke, 'Disrupting and preventing deepfake abuse: Exploring criminal law responses to AI-facilitated abuse', Chapter 29, p 587-589 in A Powell et al (eds), *The Palgrave Handbook of Gendered Violence and Technology*, 2021. See also the discussion of harms resulting from sexually explicit deepfakes in S Tong, '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.

[32] S Tong, '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] *UNSW LawJl Stus* 25 (footnotes omitted). See also: A Rizzica, *Sexually explicit deepfakes: to what extent do legal responses protect the depicted persons*, Masters Thesis, Tilburg Law School, 29 April 2021, p 16.

[33] S Tong, '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 (footnotes omitted).

[34] D Citron, Sexual privacy, *Yale LJ*, Vol 128, 2019, 1,870 at 1,884.

The harms associated with sexually explicit deepfakes were discussed in the Australian Parliament's inquiry into the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024.[35] The inquiry's report stated:

> '… [w]hile deepfake images are fake, the impacts are very real. The events depicted in the material do not need to have happened, nor do the images or videos need to be real, to cause damage to someone's life'.[36]

The inquiry's report also identified the concern that '… deepfake sexual material … can be used to harass, blackmail, and attack victims or used to extort sex acts.'[37]

Sexually explicit deepfakes that depict violence pose an additional risk of harm. The NSW Government's *NSW Sexual Violence Plan 2022–2027* 'recognises that exposure to violent pornography is among factors that increase a person's likelihood of experiencing or perpetrating sexual assault.'[38]

2.4.2 Children

Additional considerations arise where deepfake technology has been used to generate child abuse material.[39] Of foremost concern is the heightened potential for children to suffer deeper and longer-term emotional harm if they are exposed to depictions of themselves in deepfake child abuse material, given that evidence indicates that 'children are more likely than adults to lack the cognitive and behavioural capacities to understand and respond to traumatic circumstances effectively'.[40]

Concerns have also been raised that deepfake child abuse material not only harms the child victim, but also represents 'an attack on all children' because it has the potential to normalise child sexual abuse and to be used by perpetrators to groom children for child sexual abuse.[41] Further, some AI models use real child sexual abuse material to generate deepfake child abuse material, which perpetuates the harms suffered by child abuse victims as they are being further exploited to generate deepfake child abuse material.[42]

---

[35] Australian Parliament, the Senate, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024.

[36] Australian Parliament, the Senate, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 12.

[37] Australian Parliament, the Senate, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 11.

[38] NSW Government, *NSW Government Submission, Legislative Council Standing Committee on Social Issues inquiry into the impacts of harmful pornography on mental, emotional, and physical health*, November 2024, accessed 4 March 2025.

[39] Child abuse material generated by AI is also referred to as synthetic child abuse material. Illustrating the timeliness and significance of these concerns, on 1 March 2025 it was reported that a man from Queensland and a man from NSW were among 25 people charged with criminal offences as part of a global police investigation across 19 countries into AI-generated child abuse material: Australian Federal Police, Operation Cumberland - Australian duo charged as part of global investigation into AI-generated child abuse material [media release], 1 March 2025, accessed 3 March 2025.

[40] D Cruz, M Lichten, K Berg and P George, Developmental trauma: Conceptual framework, associated risks and comorbidities, and evaluation and treatment, *Frontiers in Psychiatry*, July 2022, p 1. See also: A Farrelly-Rosch and F Scanlan, *Trauma and mental health in young people*, Orygen, 2018, p 3.

[41] A Rizzica, *Sexually explicit deepfakes: to what extent do legal responses protect the depicted persons* (Masters thesis), Tilburg Law School, 29 April 2021, p 13. Justice Adams in *McEwen v Simmons* noted that 'the use of the imaginary material to groom children would make its possession more serious': *McEwen v Simmons* [2008] NSWSC 1292 at [5], (2008) 191 A Crim R 390.

[42] G Hunt and D Higgins, Deepfake AI pornography is becoming more common — what can parents and schools do to prevent it?, *The Conversation*, 12 June 2024.

The eSafety Commissioner has also noted that an increase in deepfake child abuse material is overwhelming investigating authorities, whose immediate concern is locating and rescuing the child victims shown in real child abuse material.[43]

In January 2025 the Australian Federal Police issued a warning to parents regarding an increase in the number of sexually explicit deepfakes depicting children, 'including a rise in students creating material such as deepfakes for a variety of reasons, including to harass or embarrass classmates.'[44]

2.4.3 Prevention and remediation of harms: The role of the *Online Safety Act 2021* (Cth)

The *Online Safety Act 2021* (Cth) commenced on 23 January 2022 with the object of improving and promoting the online safety of all Australians.[45] The eSafety Commissioner administers the Act. Harm prevention and harm remediation are 2 key strategies employed by the eSafety Commissioner to achieve the object of the Act.[46]

Harm prevention is promoted by industry standards and codes that require online service providers to 'take proactive steps to reduce the availability of seriously harmful online content'.[47] Basic online safety expectations state that '… social media, messaging, gaming and app services and website providers take reasonable steps to keep Australians safe online.' [48]

Harm remediation is promoted by the complaints schemes established under the Act. The complaints schemes cover a broad range of harmful online material, including sexually explicit images of adults and child abuse material. The eSafety Commissioner has stated: 'All our schemes apply to both real and synthetic material, including AI and deepfakes'.[49] Under the complaints schemes, the eSafety Commissioner has broad regulatory powers.[50] Those regulatory powers include issuing removal notices to internet service providers, which requires them to remove specified material from the internet. Failure to comply with a removal notice empowers the eSafety Commissioner to issue an infringement notice or seek civil penalties (a fine) in court. The eSafety Commissioner can also undertake regulatory action directly against an individual who posted online or threatened to post online an intimate image of another person without consent.[51] The regulatory action that can be taken includes issuing a removal notice, remedial direction, formal warning and infringement notice, and

---

[43] J Grant, *Addressing deepfake image-based abuse*, eSafety Commission, 24 July 2024, accessed 28 February 2025.
[44] Australian Federal Police (AFP), *AFP warns parents over rise in AI-generated child abuse material* [media release], 28 January 2025, accessed 17 February 2025.
[45] *Online Safety Act 2021 (Cth)*, section 3.
[46] eSafety Commissioner, Regulatory Guidance, last updated 31 January 2025. Harms relating to online bullying of adults and children are also the focus of the *Online Safety Act 2021* (Cth) and the eSafety Commissioner.
[47] eSafety Commissioner, Regulatory Guidance, last updated 31 January 2025.
[48] eSafety Commissioner, Regulatory Guidance, last updated 31 January 2025.
[49] eSafety Commissioner, eSafety Submission: Senate Standing Committee on Legal and Constitutional Affairs, Legislation Committee, Criminal Code Amendment (Deepfake Sexual Material Bill) 2024, 23 July 2024, p 2.
[50] For details of the relevant regulatory powers, see: eSafety Commissioner, *Image-Based Abuse Scheme: Regulatory Guidance*, and *Online Content Scheme: Regulatory Guidance*, last updated January 2025.
[51] Section 75 of the *Online Safety Act 2021* (Cth) provides that a person must not post online, or threaten to post online, an intimate image of another person without consent. A civil penalty of 500 penalty units ($165,000) applies. (Section 4AA of the *Crimes Act 1914* (Cth) provides that 1 penalty unit equals $330).

seeking civil penalties in court.[52] The first court proceedings instigated by the eSafety Commissioner under the Act in respect of deepfakes was *eSafety Commissioner v Rotondo* in 2023.[53]

In 2023-24 the eSafety Commissioner '…received 7,270 reports of intimate images and videos shared without consent and successfully facilitated the removal of 98% of reported conduct from 947 locations across 191 platforms'.[54]

[52] For details of the relevant regulatory powers, see: eSafety Commissioner, *Image-Based Abuse Scheme: Regulatory Guidance*, last updated January 2025.
[53] *eSafety Commissioner v Rotondo* [2023] FCA 1296.
[54] eSafety Commissioner, *eSafety Commission annual report 2023-2024*, 2024, p 170 and 173.

3. Offences

3.1 Sexually explicit deepfakes of adults

3.1.1 Commonwealth offences

In 2024 new Commonwealth offences were introduced into the *Criminal Code Act 1995* (Cth) that prohibit the use of a carriage service to transmit sexually explicit deepfakes of an adult without consent. A carriage service is a 'service for carrying communications by means of guided and/or unguided electromagnetic energy.'[55] The internet and mobile phone services are carriage services. Sending an email, texting and posting material on social media are all examples of using a carriage service. The new offences were introduced by the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* (Cth), which commenced on 3 September 2024. The Commonwealth Attorney-General, Mark Dreyfus KC MP, discussed the objects of the legislation in the Second Reading speech:

> The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 strengthens existing Commonwealth criminal offences and creates new offences to respond to the online harm caused by deepfakes and other artificially generated sexual material.
>
> Digitally created and altered sexually explicit material that is shared without consent is a damaging and deeply distressing form of abuse. This insidious behaviour is degrading, humiliating and dehumanising for victims. Such acts are overwhelmingly targeted at women and girls and perpetuate harmful gender stereotypes and gender based violence.
>
> This bill will deliver on a commitment made by the Albanese government following the National Cabinet held in May to address gender based violence. This commitment recognised the urgent and collective need to respond to the growing challenges associated with artificially generated sexual material.[56]

The 2 key offences introduced by the 2024 reforms are sections 474.17A and 474.17AA of the *Criminal Code Act 1995* (Cth).

Section 474.17A(1) prohibits a person from using a carriage service to transmit sexually explicit material of another person who is (or appears to be) 18 years of age or older without consent.[57] A maximum penalty of 6 years imprisonment applies to an offence against section 474.17A(1). The term 'material' is defined in section 473.1 to include 'material in any form, or combination of forms, capable of constituting a communication'.

Section 474.17A(2) adds that, for the purpose of the offence created by section 474.17A(1), it is irrelevant whether the material transmitted is: '(a) in unadulterated form; or (b) has been created, or altered in any way, using technology.' The following note to section 474.17A(2) clarifies that section 474.17A(1) applies to sexually explicit deepfakes:

---

[55] Dictionary to the *Criminal Code Act 1995* (Cth) and section 7 of the *Telecommunications Act 1997* (Cth).

[56] M Dreyfus, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024, Parliament of Australia, *Hansard*, 5 June 2024, p 3,723.

[57] There are exceptions to the offence created by section 474.17A(1). Those exceptions are set out in section 474.17A(3) and include: the material being transmitted for a genuine medical, scientific or law enforcement purpose; or, more broadly, where a reasonable person would consider the transmission of the material to be acceptable, having regard to such factors as the content of the material and the circumstances in which the material was transmitted.

> Paragraph (b) includes images, videos or audio depicting a person that have been edited or entirely created using digital technology (including artificial intelligence), generating a realistic but false depiction of the person. Examples of such material are "deepfakes".

Section 474.17AA provides 2 aggravated offences that also apply to sexually explicit deepfakes. The first aggravated offence is provided by section 474.17AA(1), which applies where a person commits an offence against section 474.17A(1) while subject to 3 or more civil penalty orders relating to contraventions of section 75(1) and/or section 91 of the *Online Safety Act 2021* (Cth).[58] The second aggravated offence is provided by 474.17AA(5), which applies where a person commits an offence against section 474.17A(1) and the person was responsible for the 'creation or alteration' of the material. A maximum penalty of 7 years imprisonment applies to the aggravated offences created by sections 474.17AA(1) and 474.17AA(5).

3.1.2 NSW offences

NSW has offences that prohibit the recording and distribution of intimate images, which are located in Part 3, Division 15C, of the *Crimes Act 1900*. The offences in Division 15C were introduced by the *Crimes Amendment (Intimate Images) Act 2017* to 'deter and punish the non-consensual sharing of intimate images' and to ensure that victims are 'adequately protected under the criminal law.'[59] The *Crimes Amendment (Intimate Images) Act 2017* commenced on 25 August 2017, the year in which deepfakes first appeared anonymously on Reddit.[60] Understandably, the *Crimes Amendment (Intimate Images) Act 2017* was concerned with images and videos that were recorded using smart phones or altered using standard graphic design software, rather than with deepfakes.

Case law applying, or declining to apply, NSW's intimate image offences to sexually explicit deepfakes material was not identified.[61] In the absence of case law or legislative amendment, the issue of whether these offences apply to sexually explicit deepfakes turns on the terms of the NSW provisions. Sections 91P, 91Q and 91R are the key offence provisions and section 91N defines the key terms that are used in those sections.

The term 'record' is defined to mean 'record, take or capture an image, by any means'. 'Image' means 'a still or moving image, whether or not altered'. 'Intimate image' includes 'an image that has been altered to appear to show a person's private parts, or a person engaged in a private act …'. The term 'distribute' covers distributing in person or by electronic, digital or any other means, and includes making available for viewing or access by another person.

Section 91P prohibits a person from recording an intimate image without consent. Section 91Q prohibits a person from intentionally distributing an intimate image of another person without consent. Section 91R prohibits a person from threatening to record or distribute an intimate image of another person without consent. The threat may be made by any conduct, and may be explicit or

---

[58] Section 75 of the *Online Safety Act 2021*(Cth) provides that a person must not post online, or threaten to post online, an intimate image of another person without consent. A civil penalty of 500 penalty units ($165,000) applies. (Section 4AA of the *Crimes Act 1914* (Cth) provides that 1 penalty unit equals $330). Section 91 of the *Online Safety Act 2021*(Cth) provides that a person must comply with the requirements of a removal notice, to the extent that the person is capable of doing so. A civil penalty of 500 penalty units ($165,000) applies.
[59] M Speakman, Crimes Amendment (Intimate Images) Bill 2017, *NSW Hansard*, 24 May 2017.
[60] Section 2 and 2017 (462) LW 25 August 2017.
[61] Based on a search of the Austlii database for the term 'deepfake', conducted on 3 March 2025. It should be noted, however, that such a search would only locate cases where a judgment has been published.

implicit, as well as conditional or unconditional.[62] These offences carry a maximum penalty of 3 years imprisonment and/or a fine of 100 penalty units ($11,000).[63]

Under section 91S, a court may order a person who has been found guilty of an offence against sections 91P and 91Q to take reasonable actions to remove, retract, recover, delete or destroy any intimate image that was recorded or distributed by the person in contravention of the section within a period specified by the court. A court may make a similar order in respect of a person who has been found guilty of an offence against section 91R and any intimate image threatened to be distributed by the person in contravention of that section. Contravening these orders is an offence against section 91S, which carries a maximum penalty of 2 years imprisonment and/or a fine of 50 penalty units ($5,500).

The important role currently played by NSW's intimate image offences is demonstrated by Table 3, which shows that 2,263 charges against the intimate image offences have been proven since the offences commenced in August 2017.[64] Further, the number of proven charges has been increasing each year, from 178 in 2018 to 461 in 2024. Of the total number of proven charges, 1,466 (65%) constituted a form of domestic violence (DV).

[62] Section 91T sets out certain exceptions to the offences provided by sections 91P and 91Q. These exceptions relate to conduct done for medical, scientific and law enforcement purposes. There is also an exception where a 'reasonable person' would consider the conduct acceptable, having regard to such factors as the nature and content of the image, the circumstances in which the image was recorded or distributed, and the relationship between the accused and the person depicted in the image.
[63] Section 17 of the *Crimes (Sentencing Procedure) Act 1999* provides that 1 penalty unit equals $110.
[64] NSW Bureau of Crime Statistics and Research.

Table 3: Proven charges: sections 91P(1), 91Q(1), 91R(1), 91R(2) of the Crimes Act 1900

Section	2017 (Oct-Dec)	2018	2019	2020	2021	2022	2023	2024	TOTAL
Section 91P(1)[65]	2	47	64	71	74	51	49	101	**459**
Section 91P(1) (DV)[66]	2	7	18	32	49	59	71	76	**314**
Section 91Q(1)[67]	1	19	31	32	48	34	27	31	**223**
Section 91Q(1) (DV)[68]	4	54	74	93	90	122	126	135	**698**
Section 91R(1)[69]	0	0	0	0	0	0	0	1	**1**
Section 91R(1) (DV)[70]	1	0	0	2	0	1	8	2	**14**
Section 91R(2)[71]	1	15	19	17	15	16	12	19	**114**
Section 91R(2) (DV)[72]	5	36	45	45	61	72	80	96	**440**
Total	**16**	**178**	**251**	**292**	**337**	**355**	**373**	**461**	**2,263**

Source: NSW Bureau of Crime Statistics and Research

3.1.3 Combined effect of Commonwealth and NSW offences

Following the commencement of the *Criminal Code Amendment (Deepfake Sexual Material) Act 2024* (Cth) on 3 September 2024, it is clear that the Commonwealth offences which prohibit the use of a carriage service to transmit sexually explicit material of an adult without consent also apply to sexually explicit deepfakes. But the Commonwealth offences do not apply to the creation of sexually explicit deepfakes because it is the transmission of sexually explicit material over a carriage service that is prohibited. They therefore do not address the personal and societal harms associated with the creation of sexually explicit deepfakes solely for personal gratification.

The issue of the Commonwealth offences not prohibiting the act of creating sexually explicit deepfake material was discussed by the Senate's Legal and Constitutional Affairs Legislation Committee, which noted:

> Many submitters and witnesses observed that the Bill does not criminalise the creation of deepfake sexual material as a standalone offence. The creation of the deepfake material would only be an aggravating factor under the Bill, enlivened when a person has also non-consensually transmitted the deepfake sexual material.[73]

The submission of the Australian Human Rights Commission to the parliamentary inquiry stated that prohibiting the creation of sexually explicit deepfakes was necessary to:

---

[65] Intentionally record intimate image without consent.
[66] Intentionally record intimate image without consent (domestic violence).
[67] Intentionally distribute intimate image without consent.
[68] Intentionally distribute intimate image without consent (domestic violence).
[69] Threaten to record intimate image without consent.
[70] Threaten to record intimate image without consent (domestic violence).
[71] Threaten to distribute intimate image without consent.
[72] Threaten to distribute intimate image without consent (domestic violence).
[73] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 34.

> …. recognise the violation and harms to women and other targeted persons, in the very creation of non-consensual sexual material – including for solely personal purposes. The law can also lay a strong 'foundation for education and cultural change' on non-consensual deepfake sexual material.[74]

The submission of the Commonwealth Attorney-General's Department referred to the need for Commonwealth laws to operate within the parameters set by the Australian constitution and that '…offences for the pure creation of either adult [sexually explicit] material or child sexual abuse material are typically dealt with by the states and territories'.[75]

The Senate's Legal and Constitutional Affairs Legislation Committee noted that some of the submissions it received identified that the Commonwealth offences lacked an element of threatening to create and/or distribute sexually explicit material, which could be used for sexual extortion ('sextortion'), or as a form of coercive control in a domestic violence context.[76] This gap could, however, in part be covered by the separate offence of using a carriage service to menace, harass or cause offence, under section 474.17 of the *Criminal Code Act 1995* (Cth). Section 474.17 applies where the internet or a mobile phone service has been used as the means by which to menace, harass or cause offence, but does not apply to threats delivered in person.

As to NSW's intimate image offences, it is doubtful that section 91P of the *Crimes Act 1900* (NSW) applies to sexually explicit deepfake images. As noted above (at 3.1.2), section 91P prohibits the non-consensual recording of intimate images and 'record' is defined to mean 'record, take or capture'. Sexually explicit deepfake images are altered or created, rather than recorded. If section 91P does not apply to sexually explicit deepfakes, then the non-consensual creation or production of sexually explicit deepfake images is not prohibited in NSW. This has been suggested by academics Flynn et al, who said that '… the non-consensual production or creation of a sexualised deepfake of an adult is not specifically captured' by NSW's intimate image offences.[77]

The issue then becomes whether the offences of distributing an intimate image without consent (under section 91Q) and threatening to distribute an intimate image without consent (under section 91R) would apply to sexually explicit deepfakes.

It has been suggested that NSW's intimate image offences could apply to deepfakes because they cover 'altered' images.[78] As noted above (at 3.1.2), section 91N defines an intimate image to include 'an image that has been altered …'. However, the premise that deepfakes are 'altered' images may not always be correct. As the definitions of the term 'deepfakes' in Table 1 suggest, not all deepfakes are images which have been 'altered'. In the words of the Alan Turing Institute, deepfakes '… might be

---

[74] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 35.
[75] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 36.
[76] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 37-38.
[77] A Flynn, A Powell, A Eaton and A Scott, Legal loopholes don't help victims of sexualised deepfake abuse, *360*, 3 April 2024.
[78] For instance: J Bartle, *Is it a Crime to Produce, Possess or Distribute AI Generated Child Pornography?*, Sydney Criminal Lawyers, 28 February 2023, accessed 4 March 2025; and C Woods, The spotlight cast by Taylor Swift's deepfake experience, *LSJ online*, 22 February 2024.

created from scratch, or pre-existing content may have been manipulated'. [79] The distinction, although technical, is significant. If a court finds that a sexually explicit deepfake is an intimate image which has been altered, then sections 91Q and 91R might apply. But if a court finds that a particular sexually explicit deepfake is an intimate image which has been generated or synthesised anew, then sections 91Q and 91R would not apply (unless the courts expansively define the term 'altered' to include 'generated' or 'synthesised').

Irrespective of whether sections 91Q or 91R apply to sexually explicit deepfake images in any given case, it is doubtful that the creation or production of a sexually explicit deepfake image, with all its attendant harms, is prohibited in NSW. Further, cases relating to the applicability of sections 91Q and 91R may become mired in technical details and arguments about whether every sexually explicit deepfake that is the basis of a charge in the case has been created or altered.

Moreover, NSW's intimate image offences do not prohibit conduct relating to sexually explicit deepfake audio and text. Sexually explicit deepfake audio is any audio file created by AI that contains sexually explicit material spoken in the recognisable voice of a particular person who in reality did not speak the material. Sexually explicit deepfake text is any text containing sexually explicit material that is written in the recognisable style of a particular person who in reality did not write the material. Unless other existing NSW offences apply, the creation of sexually explicit deepfake audio and text will be unprohibited in NSW if it does not involve transmission using a carriage service, as that is the point where the Commonwealth's deepfake offences apply.

3.1.4 Victoria's offences

Victoria's counterpart provisions provide a useful point of comparison, as they suggest ways in which the NSW provisions could be amended to cover sexually explicit deepfakes of adults. The Victorian provisions were introduced by the *Justice Legislation Amendment (Sexual Offences and Other Matters) Act 2022* (Vic). The Second Reading speech expressly stated that the new Victorian provisions were intended to apply to sexually explicit deepfake images:[80]

> The Bill expands the definition of 'intimate image' to include digitally created images in order to capture 'deepfake porn', where an image is generated, manipulated or altered to appear to depict the victim-survivor.

Sections 53R, 53S and 53T of the *Crimes Act 1958* (Vic) are the relevant offence provisions. Sections 53R, 53S and 53T prohibit a person from 'producing, distributing or threatening to distribute intimate images' of another person without consent, where the production or distribution of the intimate image is contrary to community standards of acceptable conduct.[81] The offences apply exclusively to sexually explicit images. Sexually explicit deepfakes that are in the form of audio or text are not within their scope. They also apply whether or not a person uses a carriage service in the commission of the offence. Each offence carries a maximum penalty of 3 years imprisonment.

---

[79] P Swatton and M Leblanc, *What are deepfakes and how can we detect them?*, The Alan Turing Institute, 7 June 2024, accessed 18 February 2025
[80] H Shing, Second Reading speech to the Justice Legislation Amendment (Sexual Offences and Other Matters) Bill 2002, *Vic Hansard*, 18 August 2022.
[81] *Crimes Act 1958* (Vic), Part 1, Division 1, Subdivision 8FAAB.

Section 53O defines the terms which inform the application of the offence provisions. 'Intimate image' is defined to mean an 'image' depicting a person in various sexualised contexts or ways. Significantly, an 'image' may be:

> (a) still, moving, recorded or unrecorded; and
>
> (b) digitally created by —
>
> > (i) generating the image; or
> >
> > (ii) altering or manipulating another image.

To 'produce' an image means to film, record, take or otherwise capture the image, or to digitally create the image.

The combined effect of the definitions of 'image', 'intimate image' and 'produce' is that Victoria's intimate image offences cover sexually explicit deepfakes that were produced either by altering an existing image or by synthesising or generating a new image. The Victorian offences also fill the gap left by the application of the Commonwealth offences being contingent on the use of a carriage service, as they apply irrespective of whether a carriage service was used in the offending. However, as noted, they do not cover sexually explicit deepfakes in the form of audio or text.

3.1.5 Other developments

The South Australian Government is proposing to introduce offences relating to sexually explicit deepfakes. The South Australian proposal resulted from the *Report of the Select Committee on Artificial Intelligence*. Recommendation 14 of the Select Committee's report called for the South Australian Government to '[r]eview the applicability and suitability of current criminal law and privacy laws in relation to AI-enabled image-based abuse (i.e. 'deepfakes')'. On 17 October 2024 the Summary Offences (Artificially Generated Content) Amendment Bill 2024 (SA) was introduced into the South Australia Legislative Council by the South Australian Government.[82]

On 22 January 2025, the United Kingdom Government announced that is proposing to criminalise the act of 'intentionally creating a sexually explicit deepfake without consent, and either with intent to cause alarm, humiliation, or distress, or for the purpose of sexual gratification and without reasonable belief in consent'.[83] It was noted in the announcement that recent amendments have already made it an offence to 'share or threaten to share intimate images, including deepfakes'.[84]

---

[82] Government of South Australia, *Deepfakes in South Australia*, n.d., accessed 31 March 2025; Government of South Australia, *Deepfakes* (Discussion Paper), August 2024; Summary Offences (Artificially Generated Content) Amendment Bill 2024 (SA) (Second Reading adjourned on 17 October 2024, as at 23 April 2025).

[83] S Sackman KC MP, Better protection for victims thanks to new law on sexually explicit deepfakes [media release], United Kingdom Government, 22 January 2025, accessed 23 April 2025.

[84] S Sackman KC MP, Better protection for victims thanks to new law on sexually explicit deepfakes [media release], United Kingdom Government, 22 January 2025, accessed 23 April 2025.

3.2 Deepfake child abuse material

3.2.1 Commonwealth offences

Commonwealth child abuse material offences are located in Division 474, Subdivision D, of the *Criminal Code Act 1995* (Cth). Subdivision D is titled 'Offences relating to the use of a carriage service for child abuse material'.[85]

Case law applying, or declining to apply, the offences in Subdivision D to deepfake child abuse material has not been identified.[86] However, in *R v Edwards* the offender was convicted of Commonwealth child abuse material offences where a majority of the child abuse material was described as 'Computer Generated Images (CGI)'.[87] Moreover, the 2024 inquiry of the Australian Parliament into the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 stated that the scope of the existing Commonwealth child abuse material offences is broad enough to encompass deepfake child abuse material:

> Material depicting persons under the age of 18 will continue to be criminalised in the Criminal Code under the existing child abuse material provisions, including child abuse material generated by AI …[88]

On 1 March 2025 the Australian Federal Police stated that they had charged 2 men with Commonwealth child abuse material offences for possessing and accessing deepfake child abuse material.[89] The 2 offences with which the alleged offenders were charged, both of which are located in Subdivision D, were sections 474.22 and 474.22A of the *Criminal Code Act 1995* (Cth). Section 474.22 prohibits 'using a carriage service for child abuse material' and 474.22A prohibits 'possessing or controlling child abuse material obtained or accessed using a carriage service'. Although not used in this particular case, another important Commonwealth offence is section 474.23, which prohibits 'possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service'. These offences all carry a maximum penalty of 15 years imprisonment.

The basis on which the existing Commonwealth offences on child abuse material in Subdivision D are said to apply to deepfake child abuse material is the broad definition of 'child abuse material' in section 473.1 of the *Criminal Code Act 1995* (Cth). For instance, the term 'material' includes 'material in any form, or combination of forms, capable of constituting a communication'. The term 'depict' includes 'contain data from which a visual image (whether still or moving) can be generated'. The

---

[85] There are other child abuse material offences in the *Criminal Code Act 1995* (Cth), such as section 417.19 (using a postal or similar service for child abuse material). There are limited defences to these offences set out in section 474.24, which essentially relate to law enforcement and online safety purposes.

[86] Based on a search of the Austlii database for the term 'deepfake', conducted on 3 March 2025. It should be noted, however, that such a search would only locate cases where a judgment has been published.

[87] *R v Edwards* [2019] QCA 15. The offence was section 474.19(1) of the *Criminal Code Act 1995* (Cth), which has since been repealed. It used the term 'child pornography material', while the current offences use the term 'child abuse material'.

[88] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 6, citing a submission from the Commonwealth Attorney-General's Department.

[89] Australian Federal Police, *Operation Cumberland - Australian duo charged as part of global investigation into AI-generated child abuse material* [media release], 1 March 2025, accessed 3 March 2025. The Australian Federal Police noted that '[a]lthough the children depicted in this material are not real, these criminal networks are still involved in the sexual exploitation of children.'

term 'describe' includes '… contain data from which text or sounds can be generated.' The term 'child abuse material' includes material which:

- 'depicts or describes a person or representation of a person' who 'is, or appears to be', under 18, and
- 'is, or appears to be', the victim of torture, cruelty or physical abuse, or
- 'is or appears to be', engaged in sexual activity.

3.2.2 NSW offences

NSW has offences on child abuse material located in Part 3, Division 15A, of the *Crimes Act 1900.* The most relevant offence is section 91H(2) of the *Crimes Act 1900*, which states that a 'person who produces, disseminates or possesses child abuse material is guilty of an offence.'[90] Section 91H(2) carries a maximum penalty of 10 years imprisonment. The use of the internet is not an element of the offence against section 91H(2).

The terms 'produce', 'disseminate' and 'possess' are defined in section 91H(1). The term 'material' is defined in section 91FA and the term 'child abuse material' is defined in section 91FB.

The term 'produce' is broadly defined to include 'film, photograph, print or otherwise make child abuse material' or 'alter or manipulate any image for the purpose of making child abuse material'. The term 'possess' includes being in possession or control of data, while the term 'disseminate' includes to 'send, supply, exhibit, transmit or communicate it to another person'.[91]

The term 'material' is broadly defined to include 'any film, printed matter, data or any other thing of any kind (including any computer image or other depiction)'. The term 'child abuse material' is defined to include material that depicts or describes a 'person who is, or appears to be or is implied to be' a child who is the victim of torture, cruelty or physical abuse, or involved in a sexual pose or activity.

Case law applying, or declining to apply, NSW child abuse offences to deepfake child abuse material was not identified.[92] However, there are 2 cases which indicate that NSW's child abuse material provisions could apply to deepfake child abuse material. In the first case, *McEwen v Simmons*, the court dismissed an appeal against a conviction for possessing child abuse material that took the form of a cartoon.[93] Justice Adams stated that the magistrate who heard the case at first instance correctly interpreted the word 'person' to include fictional or imaginary characters.[94] In the second case, *R v Jarrold*, the offender was convicted for producing child abuse material that took the form of

[90] There are limited defences and exceptions to this offence set out in sections 91HA and 91HB, which relate to such factors as law enforcement, research, public interest and, in certain limited instances, where the child abuse material was possessed by a person under 18 years of age.
[91] For a discussion of the NSW provision, see: J Bartle, *Is it a Crime to Produce, Possess or Distribute AI Generated Child Pornography?*, Sydney Criminal Lawyers, 28 February 2023, accessed 4 March 2025.
[92] Based on a search of the Austlii database for the term 'deepfake', conducted on 3 March 2025. It should be noted, however, that such a search would only locate cases where a judgment has been published.
[93] *McEwen v Simmons* [2008] NSWSC 1292; (2008) 191 A Crim R 390.
[94] *McEwen v Simmons* [2008] NSWSC 1292 at [41]; (2008) 191 A Crim R 390.

spoken and written statements made by the offender that described instances of child abuse.[95] The court stated that, for the purpose of the child abuse material offences, '[w]hether or not the material discussed in the communications was the result of fantasies or accounts of actual events was irrelevant.'[96]

3.2.3 Combined effect of Commonwealth and NSW offences

The courts have noted that the distinguishing feature between Commonwealth and NSW child abuse material offences is that the '…vice attacked by the Commonwealth legislation is the use of the internet to access the market for child pornography and the consequent boost to that market of which internet access is such an important element.'[97] In contrast, the NSW child abuse material offences apply irrespective of whether the internet or any other carriage service has been used.[98]

In the absence of an authoritative judgment of the courts, or legislative amendment that expressly clarifies the issue, an analysis of the applicability of existing child abuse material offenses to deepfake child abuse material is necessarily provisional. Nevertheless, based on the discussion of the provisions in sections 3.2.1. and 3.2.2, it is reasonable to suggest that the Commonwealth and NSW offences would apply where the internet has been used for the offending. In respect of the Commonwealth offences, this was the position of the Senate's Legal and Constitutional Affairs Legislation Committee.[99] It is also suggested by the broad definition of the terms 'material', 'child abuse material', 'depict' and 'describe'. For instance, a deepfake child abuse video would be 'material in any form, or combination of forms, capable of constituting a communication' that depicts a 'representation' of a person who 'appears to be' under 18 and who 'appears to be' the victim of torture, cruelty or physical abuse, or 'appears to be' engaged in sexual activity.

In respect of the NSW offences, their applicability to deepfake child abuse material turns on the broad definition of the terms 'produce', 'material' and 'child abuse material', 'Produce' includes to 'alter or manipulate any image' or 'otherwise make' child abuse material. Material includes 'any other thing of any kind'. 'Child abuse material' includes material that depicts or describes 'a person who is or appears to be or is implied to be' a child who is the victim of torture, cruelty or physical abuse, or involved in a sexual pose or activity. As the use of a carriage service is not an element of the offence against section 91H(2), the NSW offences would apply where the internet has not been used to produce deepfake child abuse material; such as where a smart phone is used to take a photograph of a child and software on that phone is then used to create deepfake child abuse material.

---

[95] *R v Jarrold* [2010] NSWCCA 69. At the time the offences referred to 'child pornography', rather than child abuse material. This paper uses the current term 'child abuse material'.
[96] *R v Jarrold* [2010] NSWCCA 69 at [53].
[97] *Huggett v R* [2021] NSWCCA 62 at [101].
[98] As the NSW offences also apply where the internet has been used, the unfair situation could arise where a 'double punishment' is imposed on an offender who has essentially been charged twice for the same criminality: *McEwen v Simmons* [2008] NSWSC 1292 at [2]; (2008) 191 A Crim R 390.
[99] The Senate, Legal and Constitutional Affairs Legislation Committee, *Criminal Code Amendment (Deepfake Sexual Material) Bill 2024*, August 2024, p 6, citing a submission from the Commonwealth Attorney-General's Department.

4. Conclusion

Sexually explicit deepfakes of adults are prevalent online. This is largely due to the increasing availability and decreasing complexity of the AI software that enables the creation of sexually explicit deepfakes. Sexually explicit deepfakes are a form of AI-facilitated abuse, with attendant emotional, personal and societal harms.

Deepfake child abuse material is also a concern, most recently illustrated by legal proceedings commenced by the Australian Federal Police. Existing Commonwealth and NSW child abuse material offences appear to effectively prohibit conduct relating to deepfake child abuse material, principally due to their use of broad definitions of key terms.

NSW's intimate image offences, which apply to adults, were not designed with deepfakes in mind. Those offences have, in the relatively short amount of time since 2017, become outdated due to the rapid development of deepfake technologies. The Commonwealth responded to this technological development by introducing new deepfake offences in 2024, but the Commonwealth's 2024 offences cannot do all the work in this area, as their application is contingent on the use of a carriage service.

Under the current NSW intimate image offences, the creation of sexually explicit deepfakes of adults for personal gratification is unprohibited. There are also doubts about whether in-person distribution of sexually explicit deepfakes of adults, and related in-person threats, are prohibited. These limitations could be remedied if NSW's intimate image offences were amended along the lines of the new Commonwealth and Victorian offences.

Parliament of New South Wales

Parliamentary Research Service

Sexually explicit deepfakes and the criminal law in NSW

Tom Gotsis

Research Paper No. 2025-02

ISSN 2653-8318

The NSW Parliamentary Research Service provides impartial research, data and analysis services for members of the NSW Parliament.

parliament.nsw.gov.au

Media inquiries should be directed to: media@parliament.nsw.gov.au

The Parliament of New South Wales acknowledges and respects the traditional lands of all Aboriginal people and pays respects to all Elders past and present. We acknowledge the Gadigal people as the traditional custodians of the land on which the Parliament of New South Wales stands.

This image comes from 'Our Colours of Country', which was created for the Parliament of NSW by Wallula Bethell (Munro) a Gumbaynggirr/Gamilaroi artist born and raised in Tamworth who has spent time living on Dunghutti Country and is currently living in Western Sydney on Darug Country with her husband and son.

PARLIAMENT NSW