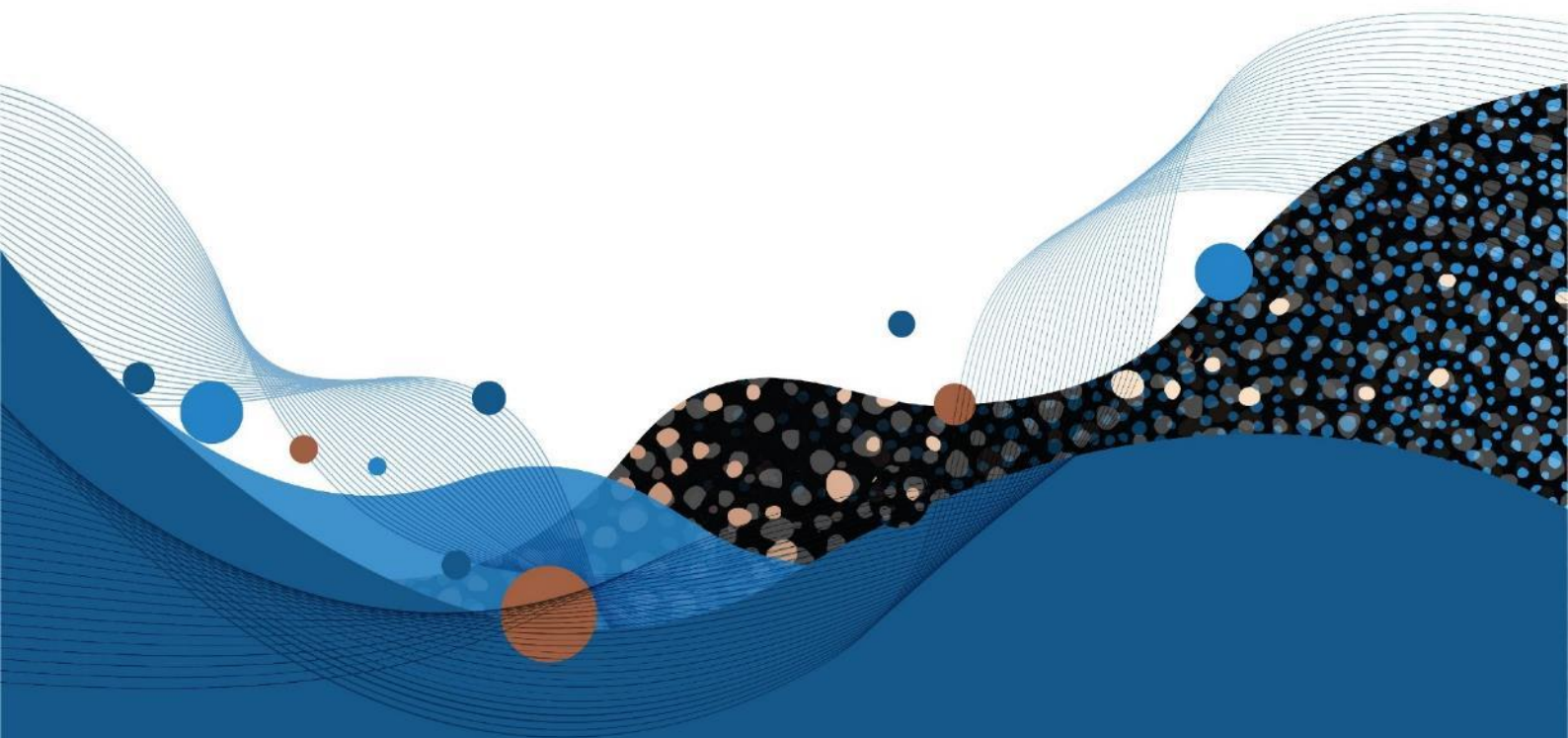


Discussion Paper

Deepfakes

August 2024



Contents

Introduction	4
Acknowledgement of Country	4
How to make a submission	4
Submissions and confidentiality	4
A message from the Attorney-General	5
Definitions	6
Deepfakes	6
Artificial intelligence	6
Background	7
Issues outside the scope of the discussion paper	8
Recent inquiries and reforms	9
Report of the South Australian Parliament Select Committee on Artificial Intelligence	9
Australian Senate Select Committee on Adopting Artificial Intelligence	9
Statutory review of the <i>Online Safety Act 2021</i> (Cth)	10
Criminal Code Amendment (Deepfake Sexual Material) Bill 2024	10
Summary Offences (Invasive Images and Depictions) Amendment Bill 2024	11
Regulation of deepfakes in Australia	12
<i>Online Safety Act 2021</i> (Cth)	12
<i>Defamation Act 2005</i> (SA)	13
<i>Copyright Act 1968</i> (Cth)	14
Australian Consumer Law	15
Privacy laws	15
South Australian criminal offences	16
<i>Filming and sexting offences</i>	16
<i>Child exploitation material offences</i>	17
<i>Indecent material</i>	17
<i>Identity theft</i>	18
<i>Fraud and dishonesty offences</i>	19
Electoral laws	20
International approaches to the regulation of deepfakes	22
European Union	22
United States	22
Canada	23
United Kingdom	23

China	24
South Korea	24
New Zealand	24
Opportunities to address the risks and harms of deepfakes	25
Appendix 1 — Discussion questions.....	26
Help and support.....	27
Office of the eSafety Commissioner	27
Counselling and other support services.....	27

Introduction

Acknowledgement of Country

We acknowledge and respect Aboriginal peoples as the State's first peoples and nations and recognise them as traditional owners and occupants of land and waters in South Australia. Further, we acknowledge that the spiritual, social, cultural, and economic practices of Aboriginal peoples come from their traditional lands and waters, that they maintain their cultural and heritage beliefs, languages and laws which are of ongoing importance, and that they have made and continue to make a unique and irreplaceable contribution to the state.

We acknowledge that Aboriginal peoples have endured past injustice and dispossession of their traditional lands and waters.

How to make a submission

Submissions in response to this discussion paper can be made until **11 September 2024**. Individuals and organisations can make a submission (confidentially if desired) by email to LLPsubmissions@sa.gov.au.

The discussion paper poses a number of questions which are set out in **Appendix 1**. You may respond to all questions, or only those that are of interest to you. While this paper focuses on opportunities for legislative reform, you may raise any additional issues and provide comments on non-legislative matters.

You can also complete our survey on YourSAy – the survey is a simplified version of the discussion questions posed in this paper. Visit www.yoursay.sa.gov.au/deepfakes.

Submissions and confidentiality

Please be aware that, unless a request for confidentiality is made, information contained in any submission may be referred to publicly or published. Any material identified as 'confidential' is still subject to the *Freedom of Information Act 1991* and, while efforts will be made to keep the material confidential, in some circumstances, it may be disclosed under that Act.

Where the disclosure of information may identify you, attempts will be made to consult with you under the *Freedom of Information Act 1991* before the documents are disclosed.

A message from the Attorney-General

The technological capabilities of artificial intelligence (AI) are a relatively new and extremely fast-moving phenomenon that governments and other regulatory bodies all over the world are currently grappling with in efforts to harness its potential, while also protecting the community from its potential harms.

While there may be many benefits from the appropriate use of artificial intelligence, it can also be utilised in a way that causes humiliation, misinformation, or harm, such as through the use of deepfakes.

Sadly, it is becoming more and more common for us to hear of instances of AI technologies being abused in the form of non-consensual deepfakes, with recent cases of deepfake 'revenge porn' videos and images targeting female high school students, where we know that an estimated 90% of all deepfakes are pornographic in nature.

Deepfakes are also being increasingly used to intimidate, misinform, or scam people, which is not only a gross invasion of privacy, but can also cause significant emotional distress, and potential reputational and economic loss to those being targeted.

Despite the growing recognition and awareness of the potential risks and harms associated with the production and creation of non-consensual deepfakes, the use of AI technology to create this material remains largely unregulated in Australia.

This discussion paper provides an opportunity for our State to ensure that South Australia's laws remain at the forefront of technological advancements, and for stakeholders and the general public to share their ideas about these technologies.

I encourage all interested South Australians to contribute by sharing their views and experiences, and to assist the Government in ensuring our laws are fit for purpose in keeping our community safe both online and in public.



Kyam Maher MLC
Attorney-General of South Australia

Definitions

Deepfakes

Deepfakes¹ refer to images, video or audio of a real person that have been edited to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say.² It can also refer to wholly computer-generated images of humans that do not exist in real life.

Deepfakes are created by using various tools and techniques that utilise machine learning, deep learning, and artificial intelligence (**AI**), including facial recognition algorithms and artificial neural networks such as variational autoencoders (**VAEs**) and generative adversarial networks (**GANs**).

In the case of deepfake audio, a person's voice may be replicated by feeding an AI machine learning model real audio data from the person, thereby training it to mimic the person's voice.

Artificial intelligence

There is no common consensus about a single definition of AI. However, it is generally understood as a field of science that is concerned with building computers and machines that can perform tasks that would normally require human intelligence, such as learning, reasoning and problem solving.

Machine learning

Machine learning is a type of AI that involves the development of mathematical algorithms and models that allow computers to learn from data and improve their performance to recognise patterns and make predictions without being explicitly programmed to do so.³

Deep learning

Deep learning is a form of machine learning that employs deeply layered neural networks – so called because they are inspired by the interconnected neurons in a human brain – to learn complex representations from data. Deep learning is used in computer vision tasks such as image recognition, natural language processing technology such as ChatGPT, and more.⁴

Generative artificial intelligence

Generative artificial intelligence is a field of AI that focuses on enabling computers to interpret and understand meaningful information about the world using visual input such as images, video, and other visual sensor data. Examples of applications for computer vision include facial recognition on smartphones, autonomous vehicle technology, object detection in manufacturing processes, analysis of medical images, and more.⁵

¹ The term deepfakes is a portmanteau of “deep learning” and “fake”. It first appeared as the username of a Reddit poster who initially used this form of content online in 2017. However, the technology that underpins deepfakes has been studied in academia since the 1990s.

² eSafety Commissioner, ‘Deepfake trends and challenges — position statement’, accessed at: <https://www.esafety.gov.au/industry/tech-trends-and-challenges/deepfakes>.

³ Parliament of South Australia, Select Committee on Artificial Intelligence, [*Report of the Select Committee on Artificial Intelligence*](#) (14 November 2023), p 13.

⁴ Ibid.

⁵ Ibid.

Background

While the alteration of images is not new, recent advances in AI capability have made it easier than ever before to create artificially generated content, like deepfakes, that are hyper-realistic and almost impossible to distinguish from real images and videos.

Deepfake technology is widely used in the creation of non-consensual pornography with an estimated 90 per cent of deepfakes being pornographic in nature.⁶ AI is being increasingly used to create non-consensual pornographic deepfakes, and there is growing awareness and recognition of pornographic deepfakes as a form of image-based sexual abuse or image-based sexual exploitation.

Increasing concerns have been raised about the potential misuse of deepfake technology, such as the creation of child exploitation material, non-consensual pornographic material (sometimes called “revenge porn”) malicious hoaxes, bullying and fraud. Concerns have also been raised about the potential use of deepfake technology to harass, intimidate, threaten, blackmail, or extort victims, particularly domestic and family violence survivors. More broadly, deepfakes may also be used to spread disinformation or to manipulate public opinion.

There is growing awareness and recognition of the real-world harm that the creation and distribution of non-consensual deepfakes can have on the depicted person, including significant emotional distress, anxiety, depression, invasion of privacy, as well as potential reputational and economic loss.

Despite growing recognition and awareness of the potential risks and harms associated with the creation and distribution of non-consensual deepfakes, the use of AI technology to create this content is largely unregulated in Australia. The use of deepfakes and AI technology remains a complex and emerging issue which presents a number of regulatory and enforcement challenges to governments.

This purpose of this discussion paper is to:

- provide an overview and examination of the existing laws in Australia, at the Commonwealth and State level, which apply to the creation and non-consensual distribution of deepfakes;
- seek views on whether existing laws in South Australia are adequate to address the potential risks and harms posed by the creation and non-consensual distribution of deepfakes; and
- seeks views on potential options for reform that may assist to address some of the risks and harms posed by the creation and non-consensual distribution of deepfakes.

Your feedback will be used to help inform any potential changes to existing South Australian laws.

⁶ Parliament of South Australia, Select Committee on Artificial Intelligence, [Report of the Select Committee on Artificial Intelligence](#) (14 November 2023), p 24.

Issues outside the scope of the discussion paper

The following matters are outside the scope of this discussion paper.

1. This discussion paper is limited to the creation and non-consensual distribution of deepfakes and, as such, does not address the regulation or application of AI technology more broadly.
2. This discussion paper is primarily concerned with potential options for legislative reform. Accordingly, this paper does not address other actions that could also be taken separately or in conjunction with legislative reform, including increased education about deepfake technology, industry awareness and advancement in detection technologies. However, this paper acknowledges the importance of a holistic approach in safeguarding against the risks and harms posed by the creation and non-consensual distribution of deepfakes.
3. While this discussion paper provides an overview of existing Commonwealth and South Australian laws that may apply to the creation and non-consensual distribution of deepfakes, this paper is focused on potential legislative changes that could be made to South Australian laws. Any potential changes to Commonwealth legislation are outside the jurisdiction of South Australia and are matters for the Commonwealth Government to appropriately consider.

Recent inquiries and reforms

As the use of deepfake and AI technology continues to grow, there have been a range of recent inquiries and reforms in Australia looking at this issue. A summary of some of the recent inquiries and reforms within South Australia and at the Commonwealth level are set out below.

Report of the South Australian Parliament Select Committee on Artificial Intelligence

On 14 November 2023, the Parliament of South Australia Select Committee on Artificial Intelligence (**Select Committee**) published the 'Report of the Select Committee on Artificial Intelligence'.⁷

The Select Committee was tasked to inquire into and report upon the current state of AI development, deployment, and application across various sectors, with a particular focus on the economic, social, and ethical implications for South Australians.

The Select Committee made 15 recommendations that are directed towards fostering the positive use of AI technology, and mitigating the risks involved with AI advancement, particularly those pertaining to privacy and image-based abuse.

Relevantly, in its report, the Select Committee queried whether current laws are adequate to protect South Australians from rogue deepfake technology. In particular, the Select Committee recommended that the South Australian Government “review the applicability and suitability of the current criminal law and privacy laws in relation to AI-enabled image-based abuse, i.e., deepfakes” (Recommendation 14).

Australian Senate Select Committee on Adopting Artificial Intelligence

On 26 March 2024, the Senate of the Australian Parliament resolved to establish the Select Committee on Adopting Artificial Intelligence (**Senate Committee**).

In accordance with its terms of reference, the Senate Committee has been tasked to inquire into and report on the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia, including consideration of:

- a. recent trends and opportunities in the development of AI technologies in Australia and overseas, in particular regarding generative AI;
- b. risks and harms arising from the adoption of AI technologies, including bias, discrimination, and error;
- c. emerging international approaches to mitigating AI risks;
- d. opportunities to adopt AI in ways that benefit citizens, the environment and/or economic growth, for example in health and climate management;
- e. opportunities to foster a responsible AI industry in Australia;
- f. potential threats to democracy and trust in institutions from generating AI; and
- g. environmental impacts of AI technologies and opportunities for limiting and mitigating impacts.

Public submissions to the Senate Committee closed on 10 May 2024. The Senate Committee is expected to report to the Australian Parliament by 19 September 2024.

⁷ Parliament of South Australia, Select Committee on Artificial Intelligence, [Report of the Select Committee on Artificial Intelligence](#) (14 November 2023).

Statutory review of the *Online Safety Act 2021* (Cth)

On 22 December 2023, the Commonwealth Minister for Communications, the Hon Michelle Rowland MP, announced the commencement of an independent statutory review into the operation of the Commonwealth *Online Safety Act 2021* (**Online Safety Act**). Ms Delia Pickard PSM has been appointed to conduct the review.

The Online Safety Act commenced in January 2022 and introduced a regulatory framework to improve and promote the safety of Australians online. The legislation provides broad powers to the online safety regulator, the eSafety Commissioner to deal with harmful online material.

The review is a broad-ranging examination of the effectiveness of the Online Safety Act and will consider whether additional protections are needed for harmful online material such as online hate and image-based abuse.

Notably, it will consider the need for further protections to address online harms stemming from new and emerging technologies like generative AI (including deepfakes) and algorithms, and whether the existing penalty regime works as an effective deterrent to industry non-compliance.

The review will also consider international developments in online safety regulation, including whether the law should be amended to impose on platforms a new duty of care towards their users, and what further steps can be taken to ensure industry acts in the best interests of children on their services.

The Commonwealth Department of Infrastructure, Transport, Regional Development, Communication and the Arts recently undertook public consultation on an issues paper regarding the review of the Online Safety Act, which opened on 29 April 2024 and closed on 21 June 2024.⁸

The issues paper sought stakeholder views on five key topics:

- Australia's regulatory approach to online services, systems and processes;
- protecting those who have experienced or encountered online harms;
- penalties, and investigation and information-gathering powers;
- international approaches to address online harms; and
- regulating the online environment, technology, and environmental changes.

Ms Pickard PSM is expected to provide a final report to the Commonwealth Government by 31 October 2024.

Criminal Code Amendment (Deepfake Sexual Material) Bill 2024

On 1 May 2024, following the meeting of National Cabinet on gender-based violence, the Prime Minister announced that the Commonwealth Government would introduce legislation to ban the creation and distribution of non-consensual deepfake pornography.

⁸ Commonwealth Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Issues Paper - Statutory Review of the Online Safety Act 2021' (April 2024), accessed at: < <https://www.infrastructure.gov.au/have-your-say/statutory-review-online-safety-act-2021>>.

The Commonwealth Attorney-General, the Hon Mark Dreyfus KC MP, subsequently introduced to the Criminal Code Amendment (Deepfakes Sexual Material) Bill 2024 (**the Deepfakes Sexual Material Bill**) to the Australian Parliament on 5 June 2024.

The Deepfakes Sexual Material Bill proposes to amend the Commonwealth *Criminal Code Act 1995* (**Criminal Code**) to strengthen offences targeting the creation and non-consensual sharing of sexually explicit material online, including material that has been created or altered using technology such as deepfakes.

Specifically, Schedule 1 of the Deepfakes Sexual Material Bill amends Part 10.6 of the Criminal Code to:

- replace the existing aggravated offence of using a carriage service to menace, harass or cause offence involving private sexual material (section 474.17A), with a new offence of using a carriage service to transmit sexual material without consent (maximum penalty of up to 6 years imprisonment)⁹;
- provide that the new offence applies to both real (non-altered) material and material that has been created or altered using technology, such as deepfake AI; and
- introduces two new aggravated offences involving the transmission of sexual material without consent (section 474.17AA), which apply where the person who transmits the material has had certain civil penalties orders made against them in relation to contraventions of the Online Safety Act, or the person has created or altered the material using technology (maximum penalty of up to 7 years imprisonment).

Summary Offences (Invasive Images and Depictions) Amendment Bill 2024

On 19 June 2024, the Hon Connie Bonaros MLC introduced the Summary Offences (Invasive Images and Depictions) Amendment Bill 2024 (**the Invasive Images and Depictions Bill**) to the South Australian Parliament.

The Invasive Images and Depictions Bill proposes to insert a new Part 5B into the *Summary Offences Act 1953* (**Summary Offences Act**) to establish new offences in relation to the creation, distribution, and threat to distribute an artificially generated invasive depiction of a person without consent. An invasive depiction, in relation to a depicted person, means artificially generated content, depicting the person in a state of undress or performing a sexual act, or other private act.

The stated Intent of the amendments' is to address concerns regarding the creation, distribution, and threat to distribute invasive depictions that have been wholly generated by AI or other digital technology.

The maximum penalties for the new offences vary between \$10,000- or 1-year imprisonment, and up to \$20,000- or 4-years imprisonment where the depicted person purports to be a real person who is under the age of 17 years.

The Invasive Images and Depictions Bill also contains amendments which propose to double the existing maximum financial penalties for the existing filming and image-based offences in Part 5A of the Summary Offences Act.

⁹ This offence applies to the transmission of sexual material that depicts a person who is, or appears to be, 18 years or older.

Regulation of deepfakes in Australia

There is currently no single piece of legislation that deals with the creation and use of deepfake technology. However, there are a number of existing legal frameworks, at both the State and Commonwealth level, that may provide relief to victims against the use and distribution of deepfakes, depending on the circumstances in which the content is created and how it is used.

This includes, but is not limited to, the Online Safety Act, defamation laws, copyright laws, the Australian Consumer Law, criminal laws (including offences in relation to image-based abuse, child exploitation material, identity theft and fraud), privacy laws, as well as electoral laws.

A brief discussion of these laws and how they may be used to regulate the use or distribution of deepfakes is provided below.

Online Safety Act 2021 (Cth)

The eSafety Commissioner has broad ranging powers under the Commonwealth Online Safety Act to deal with image-based abuse and cyberbullying, including deepfakes of this nature.

Part 6 of the Online Safety Act establishes an image-based abuse scheme, which provides the eSafety Commissioner with regulatory powers to remove and take action against the non-consensual sharing of, or threat to share, an intimate image¹⁰ online.

For the purposes of the Online Safety Act, “intimate images” may include photos and videos that have been digitally altered (for example, photoshopped images or deepfakes). They also include images or videos which have been shared in such a way as to make people think they show a specific person (for example, a nude photo tagged with a person’s name even though it is not of them).¹¹

A person who believes their intimate images have been altered and posted online can make a complaint to the eSafety Commissioner to investigate the matter.

A person who posts, or threatens to post, an intimate image may be liable to a civil penalty. The eSafety Commissioner also has powers to issue a removal notice to a provider of a social media service, relevant electronic service or designated internet service requiring the provider to remove the intimate image from the service. Removal notices can also be issued to an end-user of a social media service or a hosting service provider requiring them to remove or cease hosting the image, respectively.

Part 5 of the Online Safety Act contains a cyberbullying scheme which allows for certain people to make a complaint to the eSafety Commissioner about cyberbullying material that targets an Australian child. Part 7 of the Online Safety Act contains a cyberbullying scheme in relation to adults.

The Online Safety Act defines “cyberbullying material” to mean online communication to, or about, an Australian child that is seriously threatening, seriously intimidating, seriously

¹⁰ See Online Safety Act, s 15. An “intimate image” means a still visual image or moving visual image that shows or appears to show a person’s genitals, breasts, engaged in private activity (e.g., a person in a state of undress or engaged in sexual activity) or a person without religious or cultural attire if they would normally wear such attire in public.

¹¹ Office of the eSafety Commissioner, *Image-Based Abuse Scheme Regulatory Guidance eSG RG 2*, (updated February 2024) pg 5.

harassing or seriously humiliating. It can also include posts, comments, emails, messages, memes, images, and videos.¹²

When seeking to have cyberbullying material removed, the eSafety Commissioner may take informal or formal action. Some of these actions may include issuing an informal request to an online service provider to remove the material, giving a formal removal notice to an online service provider to remove the material, or taking other enforcement action (i.e., issuing a formal warning or seeking a court injunction).¹³

The Online Safety Act is currently the subject of an independent expert statutory review, and it is expected that a final report is due to be provided to the Commonwealth Government by October 2024. Among other things, the review will include consideration of whether additional arrangements are warranted to address online harms not explicitly captured under the existing statutory scheme, including emerging technologies such as generative AI, immersive technologies, recommender systems, end-to-end encryption, and changes to technology models such as decentralised platforms.¹⁴

Defamation Act 2005 (SA)

The tort of defamation in South Australia is largely governed by the common law¹⁵ and is modified by the *Defamation Act 2005 (Defamation Act)*.¹⁶ The stated objects of the Defamation Act include, among other things, to provide effective and fair remedies for persons¹⁷ who are harmed by the publication of defamatory matter, as well as to ensure that the law does not place unreasonable limits on self-expression and, in particular, on the publication and discussion of matters of public interest and importance.¹⁸

It is possible that the publication of a deepfake could constitute defamation in circumstances where the deepfake depicts a real person in a defamatory manner. In order to make out a cause of action for defamation, the plaintiff must establish a number of elements including:

- the communication¹⁹ was published by a person to a third party;
- the communication identified, or is about, the plaintiff;
- the communication contains imputations that are defamatory²⁰; and

¹² Office of the eSafety Commissioner, *Cyberbullying Scheme Regulatory Guidance* eSC RG 1 (updated December 2023), pg 3. See also Online Safety Act, s 6.

¹³ Office of the eSafety Commissioner, *Cyberbullying Scheme Regulatory Guidance* eSC RG 1 (updated December 2023), pg 5-10.

¹⁴ Commonwealth Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Terms of Reference — Statutory Review of the *Online Safety Act 2021* (February 2024), p 3.

¹⁵ There is also a statutory offence of criminal defamation under s 157 of the *Criminal Law Consolidation Act 1935*. Proceedings for criminal defamation may only be commenced with the consent of the Director of Public Prosecutions.

¹⁶ The Defamation Act is based on model defamation provisions which are intended to operate uniformly across Australian jurisdictions.

¹⁷ The Defamation Act also permits certain corporations (i.e., excluded corporations) to bring a cause of action for defamation, see s 9.

¹⁸ Defamation Act, s 3.

¹⁹ The communication may be achieved through many means, including spoken or written words, gestures, exclamations, or laughter, printed or electronic images, publications on the internet and communications in person or by broadcast.

²⁰ A communication is defamatory of a person if it tends, in the minds of ordinary reasonable people, to injure his or her reputation by disparaging him or her; causing others to shun or avoid him or her; or subjecting him or her to hatred, ridicule or contempt.

- the publication of the communication has caused, or is likely to cause, serious harm to the reputation of the plaintiff.

While existing defamation laws may offer victims some relief against the dissemination of deepfakes which contain defamatory imputations, one of the key challenges of bringing an action in defamation is that the burden of proof lies with the plaintiff to establish that each of the elements have been met. This can be difficult in circumstances where the plaintiff may not be able to establish who created or published the deepfake, or that the deepfake was intended to depict or identify the plaintiff.

It is also foreseeable that defendants might seek to rely upon a number of defences against a defamation action of this kind, including the defences of honest opinion and innocent dissemination. The operation of these defences may become particularly complex in circumstances where the defendant is the publisher, but not the creator of the deepfake, and may genuinely hold the honest belief that the deepfake is a true and accurate depiction of the plaintiff.

Copyright Act 1968 (Cth)

The Commonwealth *Copyright Act 1968* (**Copyright Act**) provides legal protection for people who express original ideas and information in certain forms, such as writing, visual images, moving images, music, and sound recordings.

A copyright is a legal right that gives copyright owners (usually the creator of the material) the right to control certain activities with their works, such as copying, re-using, publishing, performing, and communicating that work to the public.²¹ A copyright may be infringed if a person does one of the exclusive acts reserved to the copyright owner without that owner's permission.²²

Assuming that a deepfake has been created using original material that is subject to copyright (e.g., images, video, or audio), it is possible that the owner of the copyright may have recourse against the creator and the publisher of the deepfake for copyright infringement. The potential remedies available to the copyright owner for copyright infringement include an injunction and either damages or an account of profits.²³

Importantly, the Copyright Act provides exceptions which enable some use of copyright material without the permission of the copyright owner in certain circumstances. Amongst others, this includes "fair dealings" with copyright material for certain purposes, such as for research or study, criticism, or review, reporting of news, the giving of professional legal advice, parody and satire and making accessible format copies by, or on behalf of, a person with a disability.²⁴

²¹ Generally, a copyright lasts for 70 years after the death of the creator. However, the duration varies depending on whether the creator is known and if the work was made within the creator's lifetime. When a copyright expires, the copyrighted material falls into the public domain and may be freely used.

²² Infringement may be caused by doing any act that is comprised in the copyright, e.g., reproducing, publishing, or communicating the material. It may also be infringed by selling, hiring, or trading the copyrighted material in any way.

²³ Copyright Act, Part V Division 2, s 115.

²⁴ Copyright Act, Part III Division 3, Part IVA.

Australian Consumer Law

The Australian Consumer Law (**ACL**)²⁵ prohibits deceptive and misleading conduct in trade and commerce. The ACL may potentially offer relief for consumers who have been misled or deceived into purchasing goods or services based on artificially generated content (e.g., deepfakes) that falsely claims that the product or service has received a testimonial or been endorsed by a certain person (e.g., a celebrity or public figure) or that attributes certain characteristics to the product or service that it does not have.

Section 18 of the ACL provides that a person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive. Section 29 of the ACL also specifically protects against certain unfair practices, including where a person makes a false or misleading representation that goods or services have sponsorship, approval, performance characteristics, accessories, uses or benefits.

However, a potential limitation of the ACL in dealing with deepfakes is that it only applies in relation to false or misleading representations in relation to goods and services and therefore may not provide relief to consumers who have been misled by non-commercial deepfakes (e.g., deepfake content that is intended to harass or damage the reputation of a person rather than to sell a product or service for financial gain).

Privacy laws

The Commonwealth *Privacy Act 1988* (**Commonwealth Privacy Act**) regulates the collection, use, storage, and disclosure of personal information by some businesses and government agencies.

South Australia does not currently have specific privacy legislation although various pieces of legislation regulate the use and disclosure of information that has been obtained under that legislation. However, there are the Information Privacy Principles,²⁶ which apply as a set of binding guidelines that govern how South Australian government departments and agencies are to collect, store, use and disclose personal information.

Currently, there is no general right to privacy in Australia. However, recent developments overseas and in Australia have left open the possibility of a future tort of invasion of privacy in Australia.

In February 2023, the Commonwealth Attorney-General's Department released its final report on its review of the Commonwealth Privacy Act (**Privacy Act Review Report**).²⁷ The Privacy Act Review Report contained 116 proposals made by the Commonwealth Attorney-General's Department to amend the Commonwealth Privacy Act to better align Australia's privacy laws with global standards of information privacy protection.

²⁵ The ACL is contained in Schedule 2 of the Commonwealth *Competition and Consumer Act 2010* and applies nationally and in all States and Territories.

²⁶ South Australian Government, Department of the Premier and Cabinet, 'PC 012 Information Privacy Principles (IPPS) Instruction', accessed at: <<https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf>>.

²⁷ Commonwealth Attorney-General's Department, Privacy Act Review Report (February 2023), accessed at: <[Privacy Act Review Report | Attorney-General's Department \(ag.gov.au\)](#)>.

On 28 September 2023, the Commonwealth Government published its response to the Privacy Act Review Report (**Government Response**).²⁸

The Government Response proposes widespread reforms to the Commonwealth Privacy Act, including in-principle support for the introduction of a statutory tort of serious invasion of privacy, based on the model recommended by the Australian Law Reform Commission (**ALRC**) in its Report 123 'Serious Invasions of Privacy in the Digital Era'.²⁹

If a statutory tort of serious invasion of privacy is enacted in Australia, it is unclear to what extent it would apply to the non-consensual creation and use of deepfakes. This would likely depend on the nature and scope of any such a tort, including whether the use of a person's image, voice or likeness can properly be characterised as "private information".

South Australian criminal offences

In South Australia, there are a number of criminal offences under the *Criminal Law Consolidation Act 1935 (CLCA)* and Summary Offences Act that may capture the creation and distribution of non-consensual deepfakes, depending on the content of the deepfake and the purpose for which it is created or used.³⁰

This includes offences in relation to filming and sexting, child exploitation material, indecent material, identity theft and fraud and dishonesty. These offences are discussed in further detail below.

Filming and sexting offences

Part 5A of the Summary Offences Act sets out a number of filming and image-based sexual offences, including:

- humiliating or degrading filming — s 26B;
- distribution of invasive image — s 26C;
- indecent filming — s 26D; and
- threats to distribute an invasive image or image obtained from indecent filming — s 26DA.

Image-based offences in South Australia are currently summary offences, except where the person who is the subject of the indecent filming or the distribution of an invasive image or indecent filming is under the age of 17 years. In these circumstances, the penalty is 4 years imprisonment, making the relevant offences minor indictable.

For each of the offences in Part 5A, an "image" is defined to mean "a moving or still image" and includes "an image that has been altered by digital or other means".³¹

²⁸ Commonwealth Government, Government Response Privacy Act Review Report (September 2023), accessed at: <<https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>>.

²⁹ Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era (ALRC Report 123)' (September 2014), accessed at: <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/>>.

³⁰ For completeness, it is noted that there are also a number of Commonwealth based-offences under the Criminal Code which may apply to the creation and non-consensual distribution of deepfakes. These offences are outside the scope of this paper.

³¹ Summary Offences Act, s 26A.

An image of a person will be taken to be an “invasive image” of the person if it depicts the person in a place (other than a public place) engaged in a private act, or in a state of undress that visibly shows a person’s bare genital or anal region, or bare breasts (in the case of a female).³² “Film” has a corresponding definition and means to “take images by any means”.³³

Given that an image is already defined to include an image that has been altered by digital or other means, it is likely that a humiliating or degrading image, or an invasive image of a real person which has been altered using AI or other digital technology, would already be caught within the scope of the Part 5A offences. By its nature, the creation of a deepfake necessarily relies upon AI algorithms superimposing an existing image onto a source image of a real person to create a realistic, albeit false, depiction of that person.

Although it is less common, it is possible for artificially generated content to be created which does not rely upon an existing image or video of the depicted person. For example, it may be possible to use AI algorithms to generate a synthetic depiction of a real person using other synthetic images of that person that may still appear to be hyper-realistic. The Summary Offences Act does not expressly refer to images that may have been wholly generated by AI.

Child exploitation material offences

Part 3 Division 11 of the CLCA contains a number of offences relating to the possession, production, and dissemination of child exploitation material.

For the purposes of these offences, “child exploitation material” is defined to include material that consists of, or contains, the image or representation of (or what appears to be the image or representation of) a child under, or apparently under, the age of 17 years.³⁴

The term “material”³⁵ is, in turn, defined broadly to include any written or printed material, picture, painting or drawing, as well as any photographic, electronic, or other information or data from which an image or representation may be produced or reproduced. It also expressly includes any film, tape, disc or other object or system containing any such information or data.

Accordingly, a person who takes steps to produce child exploitation material by using AI or other digital technology to create an image, video or audio that depicts a simulated child would be caught within the scope of the existing offences. Similarly, the current provisions would also likely apply to a person who disseminates child exploitation material that has been generated using AI or other digital technology.

Indecent material

Part 7 of the Summary Offences Act also contains offences relating to the production and exhibition of offensive and indecent material which may potentially capture artificially generated content and deepfakes.

The term “material” is defined broadly for the purposes of Part 7 and relevantly includes, any picture, painting, drawing, photograph, film, video recording or other object or thing from which an image may be reproduced, as well as any computer data or computer record or system containing the data. It also includes any other material or object on which an image or representation is recorded or from which an image or representation may be reproduced.

³² Summary Offences Act, s 26A(2).

³³ Summary Offences Act, s 26A.

³⁴ CLCA, s 62.

³⁵ Ibid.

Section 33(2) of the Summary Offences Act states that it is an offence for a person to produce or take any step in the production of indecent or offensive material for the purpose of sale. It is also an offence to exhibit indecent or offensive material in a public place or to be viewable from a public place. The offence carries a maximum penalty of up to \$20,000 or imprisonment for six months.

For the purposes of the offences in Part 7 of the Summary Offences Act:

- “indecent material” is defined to mean material that is, in whole or part, of an indecent, immoral, or obscene nature; and
- “offensive material” is defined to mean material of which the subject matter is, or includes: violence or cruelty; the manufacture, acquisition, or use of instruments of violence or cruelty; the administration or use of drugs; or instruction in crime or revolting or abhorrent phenomena, and which would cause serious and general offence amongst reasonable adult members of the community.

Notably, a limitation on the operation of this offence is that s 33(6) of the Summary Offences Act provides that a prosecution for an offence against s 33 may only be brought with the written consent of the Minister.

Identity theft

Part 5A of the CLCA contains a number of offences in relation to identity theft that may apply in circumstances where a person uses a deepfake to falsely assume the identity of another person or to misuse personal identification information to obtain an unlawful benefit.

These offences include:

- assuming a false identity, or falsely pretending to have particular qualifications or to be entitled to act in a particular capacity and making a false pretence—s 144B;
- misuse of personal identification information³⁶ intending to commit or facilitate the commission of a serious criminal offence³⁷ — s 144C; and
- producing or possessing material intending to use the material, or to enable another person to use the material, for a criminal purpose³⁸ — s 144D.

The Statutes Amendment (Identify Theft) Bill 2023 (Identity Theft Bill) was introduced to the South Australian Parliament on 15 June 2023. It passed the Legislative Council on 8 February 2024 and was received in the House of Assembly on the same day but has not yet been debated in the House of Assembly.

The Identity Theft Bill contains a number of amendments that may assist to make it easier to charge and prosecute identity theft (including where deepfakes are used to commit identify theft).

³⁶ “personal identification information” includes information used to identify the person and, in the case of a natural person, relevantly includes (amongst other things): biometric data relating to the person and the person’s voice print. “Voice print” is separately defined to mean computer data recording the unique characteristics of a person’s voice.

³⁷ “serious criminal offence” means an indictable offence or an offence prescribed by regulation of the purposes of the definition.

³⁸ “Criminal purpose” is defined to mean the purpose of committing or facilitating the commission of an offence.

In particular, the Identity Theft Bill includes amendments to:

- ss 144B and 144C of the CLCA so that it will be an offence to make a false pretence, or to make use of another person's personal identification information intending to commit or facilitate the commission of *any* offence (rather than a serious criminal offence);
- s 144D of the CLCA to increase the maximum penalties from 3 to 5 years imprisonment; and
- insert new s 144DA which will make it an offence to possess personal identification information of another person without a reasonable excuse.

Fraud and dishonesty offences

There are growing reports of deepfakes being used by criminals to commit fraud and other scams to obtain a financial benefit.

In February 2024, it was reported that a multinational Hong Kong company had lost HK \$200 million (US \$25.6 million) due to a sophisticated scam using deepfake technology.³⁹ The scam involved a digitally recreated video of the company's chief financial officer, along with other employees, who appeared in a video conference call instructing an employee to transfer company funds. The scammers were able to convincingly replicate the voices of targeted individuals using publicly available video and audio footage. The scammers are reported to have followed up with the employee with emails, instant messages and one-on-one video calls over the course of a week after the video conference call.

In South Australia, fraud is a common law offence, but is supplemented by the CLCA. At common law, fraud is defined as dishonestly obtaining a benefit, or causing a loss, by deception or other means. Section 270(1) of the CLCA provides that any person who is convicted of any cheat or fraud punishable at common law is liable to be imprisoned for a term not exceeding two years.

In addition, Part 5 of the CLCA also sets out a number of offences relating to dishonesty, including the offences of:

- theft (dishonestly dealing with property without the owner's consent with intent to deprive or make a serious encroachment on the owner's property) — s 134; and
- deception (deceiving another person and, by doing so, dishonestly obtaining a benefit or causing a detriment) — s 139).

Accordingly, to the extent that deepfakes might be used in order to commit theft or deception in order to obtain a financial benefit, this conduct is likely already captured by the existing offences in the CLCA.

³⁹ Ars Technica, Benj Edwards, 'Deepfake scammer walks off with \$25 million in first-of-its-kind AI heist' (2 June 2024), available at: <[Deepfake scammer walks off with \\$25 million in first-of-its-kind AI heist | Ars Technica](#)>.

Electoral laws

Increasing concerns have been raised about the use of deepfakes and AI technology in the context of elections and the broader political sphere.

In particular, deepfakes of politicians, electoral candidates and other public political figures are being used to mislead voters into believing that the depicted person said or did something they did not. In this context, deepfakes are usually created for the purpose of causing reputational harm to the depicted person in an effort to influence voter opinion and the potential outcome of an election.

For example, in 2019, a manipulated video of Nancy Pelosi that made the US House Speaker appear intoxicated and slurring her words was spread across the internet. The video was viewed more than 2.5 million times on Facebook in a matter of days and was shared by prominent political figures.⁴⁰

The use of deepfakes and AI generated content also featured heavily in the recent Indian election in June 2024. It has been reported that political parties in India spent an estimated US\$50 million (AU\$75.2 million) on authorised AI generated content for targeted communication with their constituencies.⁴¹ In January 2024, a video of Muthuvel Karunanidhi, former chief minister of the southern state of Tamil Nadu, was shown at his party's youth wing conference. Clad in his trademark black sunglasses, white shirt, and yellow shawl he is seen in a video congratulating a friend and fellow politician on the launch of their autobiography. This is despite the fact that Karunanidhi died in 2018.⁴² Earlier this year, the Indian Prime Minister Narendra Modi addressed an audience in Hindi, which was translated into Tamil in real time by the government-created AI tool *Bhashini*.⁴³

Currently, there is no express prohibition or restriction on the use of deepfakes or artificially generated content in respect of electoral advertising, either at the Commonwealth or State level. Similarly, there is no current requirement to disclose the fact that electoral content has been created or modified by AI technology.

In South Australia, the *Electoral Act 1985* (**Electoral Act**) contains provisions relating to misleading electoral advertising which may apply to electoral advertisements that have been generated or modified by AI, including deepfakes.

Relevantly, s 113 of the Electoral Act provides that it is an offence for a person to authorise, cause or permit the publication of an electoral advertisement, if it contains a statement which claims to be fact, but is actually inaccurate and misleading to a material extent. The offence imposes a maximum penalty of \$5,000 in the case of a natural person and \$25,000 in the case of a body corporate. In circumstances where the Electoral Commissioner is satisfied that the

⁴⁰ Markus Appel, Fabian Prietzel, The detection of political deepfakes, *Journal of Computer-Mediated Communication*, Vol 27, Issue 4, July 2022, accessed at: <<https://doi.org/10.1093/jcmc/zmac008>>.

⁴¹ Vandinika Shukla, Bruce Schneier, The Conversation, 'Indian election was awash in deepfakes – but AI was a net positive for democracy' (10 June 2024), accessed at: <<https://theconversation.com/indian-election-was-awash-in-deepfakes-but-ai-was-a-net-positive-for-democracy-231795>>.

⁴² Meghna Bail, Aditya Varier, ABC News, 'Deepfakes take just minutes to make with artificial intelligence. Here's how Indian political parties use them against opponents' (30 May 2024), accessed at: <<https://www.abc.net.au/news/2024-05-30/how-ai-is-disrupting-india-election-campaign/103899138>>.

⁴³ Meryl Sebastian, BBC, 'AI and deepfakes blur reality in India elections' (16 May 2024), accessed at: <<https://www.bbc.com/news/world-asia-india-68918330>>.

electoral advertisement contains this breach, the Commissioner may request the advertiser withdraws the advertisement or publishes a retraction.

It could be argued any artificially generated content that falsely depicts a particular politician or prospective political candidate claiming to express a particular view or belief, as a statement of fact, is inherently misleading and inaccurate. However, whether such an electoral advertisement is likely to be misleading and inaccurate to a material extent, is likely be a question of fact and degree.

International approaches to the regulation of deepfakes

International jurisdictions have taken a number of different approaches to regulating the creation and use of deepfakes.

Some jurisdictions have taken a broad regulatory approach by imposing certain disclosure or labelling requirements on their use, while others have chosen to enact criminal offences to expressly prohibit or ban the use of deepfakes of a particular kind (e.g., pornographic deepfakes) or in a particular context (electoral campaigns).

Alternatively, some jurisdictions have taken a comprehensive systems-based approach to regulating the use of AI across all environments, while many jurisdictions have yet to take any specific action.

European Union

On 13 March 2024, the European Parliament adopted the *Artificial Intelligence Act (AI Act)*. The Act was formally approved by the European Council on 21 May 2024.⁴⁴ The AI Act establishes obligations for AI systems, based on their potential risks and level of impact.

Under the framework established by the AI Act, AI systems that present an “unacceptable” risk will be prohibited. AI systems that present a “high risk” will be subject to regulatory requirements to gain access to the European Union market, while those that present a limited or minimal risk will be subject to lesser information and transparency requirements.

In addition, the AI Act will impose requirements for artificial or manipulated images, audio or video content generated using AI systems to be clearly labelled.

The legislation imposes fines for infringements of the AI Act, which are set as a percentage of the offending company’s global annual turnover in the previous financial year, or a predetermined amount, whichever is higher.

The European Parliament’s approach to regulate online service providers that host AI systems (rather than the individual end-user) is the first of its kind in the world and is a significant step forward in regulating the complexities and capabilities of AI systems.

United States

There is currently no express federal legislation that governs the creation or use of deepfakes in the United States (**US**).

In 2019, the US Congress passed the *National Defence Authorization Act*, which requires the Director of National Intelligence to report on the use of deepfakes by international governments, its ability to spread misinformation, and its potential impact on national security. In 2023, the *DEEPFAKES Accountability Act* was introduced as a private members bill to the US House of Representatives.⁴⁵ The stated objective of the Act is to combat the spread of disinformation through restrictions on deep-fake video alteration technology. The Act requires

⁴⁴ European Council, Council of the European Union, ‘Artificial intelligence (AI) Act: Council gives final green light to the first worldwide rules on AI’ (21 May 2024), accessed at: <[Artificial intelligence \(AI\) act: Council gives final green light to the first worldwide rules on AI - Consilium \(europa.eu\)](https://www.consilium.europa.eu/en/press/press-releases/2024/05/21-artificial-intelligence-act/)>.

⁴⁵ Known as the “Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act” or the “DEEPFAKES Accountability Act”. See US Congress, Text – H.R.5586 – 118th Congress (2023-2024): DEEPFAKES Accountability Act, accessed at: <<https://www.congress.gov/bills/118/congress-house/bills/5586/text>>.

people who create and distribute deepfakes to comply with certain obligations. Namely, deepfakes that contain altered images or visual elements are required to include an embedded digital watermark that identifies them as such, while audio recordings that contain altered audio must include a verbal disclosure at the start of the recording, declaring that they contain altered audio.

In 2024, the bipartisan *DEFIANCE Act* was introduced to the US Senate to establish civil remedies for victims of deepfake pornography, prompted by falsified sexually explicit images of Taylor Swift circulating online.⁴⁶

A number of US states have enacted laws regulating the use of deepfake technology. In 2019, Texas passed legislation banning the use of deepfakes to influence elections. That same year, California introduced laws making it illegal to distribute deepfakes of political candidates, within 60 days prior to an election.

Since then, California has also enacted laws banning pornographic deepfakes made without consent and Georgia and Virginia have enacted laws banning the unlawful distribution of sexually explicit deepfakes.

In 2020, New York passed laws establishing rights for legal action against the unlawful publication of deepfakes.

Canada

In Canada, the distribution of non-consensual intimate images is currently prohibited, however there appears to be some doubt about whether these laws are sufficient to capture sexually explicit deepfakes.⁴⁷ Canada is also reportedly exploring the possibility of new legislation that would make it illegal to create and distribute deepfakes with malicious intent.

United Kingdom

The United Kingdom (UK) has introduced several initiatives to address the threat of deepfakes, including funding research into deepfake detection technologies, and partnering with industry and academic institutions to develop best practices for detection and response.

In 2023, the UK Parliament passed the *Online Safety Act*, which came into operation on 26 October.⁴⁸ The Act establishes a new regulatory regime to address illegal and harmful content online. Amongst other things, the *Online Safety Act 2023* added a new provision to the UK *Sexual Offences Act 2003*, spelling out that images created or altered by computer graphics, or any other method, fall within the definition of photograph or film. It also added in a provision concerned with the sharing of, or threatening to share, intimate photographs or film: the words “appears to show” another person in an intimate state.

⁴⁶ Referred to as the “Disrupt Explicit Forged Images and Non-Consensual Edits Act” or “DEFIANCE Act”. See US Congress, Text – S.3696 – 118th Congress (2023-2024): DEFIANCE Act, accessed at: <<https://www.congress.gov/bill/118th-congress/senate-bill/3696/text>>.

⁴⁷ The Canadian Bar Association, ‘[We are not ready for deepfakes: How Canadian privacy torts do not adequately address the unique harm posed by targeted deepfakes](#)’ (3 October 2023).

⁴⁸ UK Government, Department for Science, Innovation & Technology, Online Safety Act: explainer (8 May 2024), accessed at: <<https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>>

The UK Government has also recently announced that it will progress separate legislative amendments to make maliciously creating a sexually explicit deepfake of an adult, a specific criminal offence.⁴⁹

China

In 2019, the Chinese Government introduced new laws, known as the “Deep Synthesis Provisions”, that require individuals and organisations to disclose when they have used deepfake or other deep synthesis technology in media. The laws also prohibit the distribution of deepfakes without a clear disclaimer that the content has been artificially generated.⁵⁰

South Korea

In 2020, South Korea introduced laws making it an offence to distribute deepfakes that could “cause harm to the public interest”. In 2023, South Korea introduced legislation to ban the use of AI-generated deepfake videos in election campaigns within 90 days prior to an election.

The South Korean Government has recently announced plans to comprehensively restructure its copyright system for AI-generated content, to address the spread of fake news created by deepfake technology.⁵¹ The new policies will aim to establish a digital framework that ensures the protection and advancement of digital rights, including a proposal to mandate the use of watermarks on AI-generated content.

New Zealand

In New Zealand, the *Harmful Digital Communications Act 2015 (HDC Act)* aims to deter, prevent, and mitigate harm caused to individuals by digital communications, and to provide victims with a quick and efficient means of redress.

Section 22A of the HDC Act makes it an offence for a person, without reasonable excuse, to post a digital communication that is an intimate visual recording of someone else, without their consent. The offence carries a maximum penalty of up to \$50,000- or 2-years imprisonment in the case of a natural person, and a fine of up to \$200,000 in the case of a body corporate.

An intimate visual recording includes a photo, video or digital image that is made in any medium using any device, and includes recordings of a sexual nature, such as where the person is naked, engaged in sexual activity or in a state of undress. On its face, it appears that the HDC Act would capture the non-consensual posting of sexually explicit deepfakes. However, there appears to be some doubt about the extent to which deepfakes may be captured under the HDC Act.⁵²

⁴⁹ Ibid.

⁵⁰ The Diplomat, Asha Herajani, ‘China’s new legislation on deepfakes: should the rest of Asia follow suit?’ (8 March 2023), accessed at: <<https://thedi diplomat.com/2023/03/chinas-new-legislation-on-deepfakes-should-the-rest-of-asia-follow-suit/>>.

⁵¹ Dig Watch, DW Team, ‘South Korea announces plan for AI copyright and deepfake management’ (21 May 2024), accessed at: <<https://dig.watch/updates/south-korea-announces-plan-for-ai-copyright-and-deepfake-management>>.

⁵² Newshub, Molly Swift, ‘Australia criminalises AI nudes – should NZ do the same?’ (8 June 2024), accessed at: <<https://www.newshub.co.nz/home/politics/2024/06/australia-criminalises-ai-nudes-should-nz-do-the-same.html>>.

Opportunities to address the risks and harms of deepfakes

While there are a wide range of existing South Australian and Commonwealth laws that may provide relief to people whose images or voice have been used in a deepfake without their consent, there is currently no express legal framework which comprehensively regulates the creation and use of deepfakes in Australia.

As the development and use of deepfake and AI technology continues to progress at an unprecedented rate, it is vital that South Australia's laws keep pace with the emerging risks and harms posed by this type of content. The use of deepfake technology to perpetuate image-based abuse and exploitation is of particular concern.

While acknowledging the unique regulatory and enforcement challenges posed by deepfake technology, there are potential options for legislative reform that may assist to address some of the risks and harms posed by the creation and non-consensual use of deepfakes.

Some of the potential options for legislative reform could include:

- reviewing and strengthening existing South Australian criminal offences to ensure that, where possible, they expressly capture deepfakes and other artificially generated content where this is considered necessary or desirable;
- prohibiting or imposing restrictions on the creation and non-consensual distribution of deepfakes and artificially generated content of a particular kind (e.g., sexually explicit deepfakes) or in particular settings (e.g., electoral campaigning);
- exploring options to establish a new criminal offence to expressly capture the creation and non-consensual distribution of deepfakes in certain circumstances, such as where the deepfake depicts a real person and there is an intent to cause harm, where the depiction is likely to cause serious offence based on generally accepted community standards, or unless the content contains a watermark or other disclosure that identifies that the content has been artificially generated or contains artificially generated elements; or
- exploring options to establish a new civil tort based on the principles of copyright, intellectual property and privacy law that would make it unlawful for a person to use another person's image or voice in the creation or use of artificially generated content without consent.⁵³

This paper sets out a number of discussion questions at **Appendix 1** on which your feedback is sought.

The questions seek feedback on a range of issues raised in the discussion paper, including views on potential legislative options that may address some of the risks and harms that have been identified in relation to deepfakes.

Your feedback will help inform any potential changes to existing South Australian laws.

⁵³ Some states in the US have enshrined rights of publicity. The right of publicity (sometimes referred to as misappropriation) is a legal action that prohibits the use of another person's name, image, likeness, or voice without their consent, particularly if that use is for commercial purposes.

Appendix 1 — Discussion questions

This discussion paper poses a number of questions. You may respond to all questions, or only those that are of interest to you.

While this paper focuses on opportunities for legislative reform, you may raise any additional issues and provide comments on non-legislative matters.

Discussion questions

1. Do you think there is a need to regulate the creation and use of deepfakes?
2. If so, in what circumstances do you think the creation and use of deepfakes should be regulated? How should deepfakes be regulated in these circumstances?
3. What are the benefits of regulating the creation and use of deepfakes?
4. What are the risks or challenges of regulating the creation and use of deepfakes?
5. Are there any circumstances where the creation or distribution of deepfakes should be prohibited? If so, why?
6. Is there a need to change any of South Australia's existing criminal offences, or their application, to address the creation or use of deepfakes? If so, what changes should be made?
7. Do you consider there to be a gap in the way South Australia's laws currently apply to deepfakes? If so, in what way do you think this gap should be addressed?
8. Do you think there is a need to create a new criminal offence or civil tort that expressly deals with the creation and non-consensual use of artificially generated content that depicts a real person? Why/why not?
9. Are there any other ways in which you think South Australia's laws could be strengthened or improved to address the creation and use of deepfakes?

Help and support

Office of the eSafety Commissioner

Australians whose images or videos have been altered and posted online can contact the Office of the eSafety Commissioner for help to have them removed.

The Office of the eSafety Commissioner investigates image-based abuse which means sharing, or threatening to share, an intimate photo or video of a person online without their consent. This includes intimate images that have been digitally altered like deepfakes.

The Office of the eSafety Commissioner can also help to remove:

- online communication to or about a child that is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating - known as cyberbullying;
- illegal and restricted material that shows or encourages the sexual abuse of children, terrorism, or other acts of extreme violence.

You can find out more information about reporting harmful online content to the Office of the eSafety Commissioner at: <https://www.esafety.gov.au/report>

Counselling and other support services

1800RESPECT

Confidential counselling, support and information for people affected by sexual abuse or domestic and family violence. Available 24/7.

Phone: 1800 737 732

Website: <https://www.1800respect.org.au/>

Kids Helpline

5- to 25-year-olds. All issues. Confidential phone counselling available all day, every day. Online chat available 24/7, 365 days a year.

Phone: 1800 55 1800

Online chat: <https://kidshelpline.com.au/get-help/webchat-counselling>

Lifeline

All ages. All issues. Phone counselling and online chat available all day, every day.

Phone: 13 11 14

Website: <https://www.lifeline.org.au/>