Northern Ireland Assembly

Research and Information Service
Briefing Paper

Paper 01/22 January 2022 NIAR 02-22

# Cyberflashing and Deepfake Pornography

**Georgina Ryan - White**

## 1 Introduction

This briefing paper provides information in response to the Committee for Justice's research request about practices in other jurisdictions to address criminalising deepfake pornography and cyberflashing. This information will inform the Committee's consideration of the Sexual Offences (Victims and Trafficking) Bill. The paper provides analysis of internet law as a reserved matter in the context of the Online Safety Bill currently progressing through the UK Parliament. It also looks at how other jurisdictions have legislated for these types of behaviours.

This paper is divided into the following sections:

- Section 1 provides a brief introduction;
- Section 2 provides background and context;
- Section 3 examines internet law and regulation as a reserved matter
- Section 4 summarises UK wide developments to date; and
- Sections 5 to 10 provide an overview of legislative arrangements and practices in other jurisdictions.

# 2 Background and Context

## *2.1 Cyberflashing*

The term cyberflashing is used to refer to a range of behaviours, which most commonly involves a man sending an unsolicited picture of his genitals to a woman.[1] Cyberflashing can be distinguished from other forms of intimate image abuse where the victim is the subject of the image. With cyberflashing, the victim is not the subject of the image but rather the recipient.

In practice, recipients of cyberflashing often do not know the identity of the sender, with pictures or video recordings being sent via peer-to-peer methods such as AirDrop[2], rather than via a telephone network or the internet. As such, a sender can be both anonymous and proximate. However, cyberflashing may take other forms. It is prevalent on certain dating apps and social media, and can also take place between people who may know each other.

There is a shortage of data to indicate the extent of cyberflashing perpetration and victimisation, although research in this area is now starting to emerge.[3] It appears that cyberflashing is commonly experienced by many people, 'with women, and young women in particular, disproportionately facing the highest rates of victimisation and disclosing the most negative impacts'.[4] A YouGov survey in 2018 found that 41% of women had been sent an unsolicited penis picture; for younger women, this rose to almost half of women aged 18-24 (47%).[5]

It has been highlighted that 'gaps in knowledge about cyberflashing' include men's experiences of the behaviour. Marcotte et al's survey of gay and bisexual men 'indicated a high incidence of being sent unsolicited genital images, but only a small minority of men disclosed negative impacts. The authors argue women's experiences are best understood within the broader context of men's sexual violence against women, which might be of less direct relevance to the experiences of male sexual minorities.'[6]

Currently 'exposure' is an offence under Article 70 of the Sexual Offences (Northern

[1] Law Commission (2021) HC547 Modernising Communications Offences A final report, pg 233: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/07/Modernising-Communications-Offences-2021-Law-Com-No-399.pdf

[2] Apple phones have an AirDrop facility, meaning a phone nearby can request to send an image to another if it has open settings.

[3] C McGlynn and K Johnson (2020) Criminalising Cyberflashing: Options for Law Reform, The Journal of Criminal Law: https://journals.sagepub.com/doi/10.1177/0022018320972306

[4] Ibid

[5] YouGov, 'Four in Ten Female Millennials Have Been Sent an Unsolicited Penis Photo' (2018) <https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic>

[6] AS Marcotte and others, 'Women's and Men's Reactions to Receiving Unsolicited Genital Images from Men' (2020) J Sex Res 1 as cited by C McGlynn and K Johnson at 3.

Ireland) Order 2008:

**Exposure**

**70.**—(1) A person commits an offence if—

(a)he intentionally exposes his genitals, and

(b)he intends that someone will see them and be caused alarm or distress.

(2) A person guilty of an offence under this Article is liable—

(a)on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum or both;

(b)on conviction on indictment, to imprisonment for a term not exceeding 2 years.[7]

However, it is unclear whether exposure of genitals online falls within this provision.[8] The Law Commission for England and Wales examined the similar offence of exposure under section 66 of the Sexual Offences Act 2003. It noted that:

> *[…] there are two factors that limit the applicability of section 66 to cyberflashing. The first problem, as we noted in our consultation paper, is that it is not clear that section 66 would cover "non-live" instances of cyberflashing (ie photographs or recordings). Whilst some acts of exposure that take place online are live – such as an act of exposure over a video-calling facility – a significant proportion of the offending behaviour constituting cyberflashing is not live, instead involving photographs or pre-recorded video.*
>
> *The second limiting factor relates to the genitals exposed: specifically, whether they are the genitals of the person exposing them. That the exposed genitals are those of the exposer would seem to be the sine qua non of exposure; a person doesn't "flash" using someone else's genitals. In any case, it is a requirement of the section 66 offence, and not one liable to particularly tricky problems of proof. However, when images of genitals are sent to another, as in the case of cyberflashing, it may be neither obvious nor significant that the genitals are those of the sender. The harm experienced does not correlate with any sure knowledge that the image is that of the sender; indeed, in many if not most cases of cyberflashing, the recipient will have no idea whether the genitals in the image belong to the sender. Yet the harm is the same. Further, it may be difficult or impractical to require proof as to this matter. In this sense, cyberflashing differs*

[7]The Sexual Offences (Northern Ireland) Order 2008, Article 70: https://www.legislation.gov.uk/nisi/2008/1769/article/70

[8] Ibid at 3

*from "flashing" in the traditional sense.*[9]

## *2.2 Deepfake Pornography*

Deepfake is a blend of the words 'deep learning' and 'fake' and describes the hyper-realistic digital falsification of images, video, and audio.[10] Deepfake pornography is the use of deepfake techniques to create pornographic photos or videos, often using the facial features of someone represented in non-sexual images to add on to the body of someone appearing in a pornographic photo or video.[11] Individuals whose faces are used are the primary victims of deepfake pornography as are those appearing in pornographic material used to make deepfake pornography as they will not have not consented to their bodies being used for that purpose.

The making and sharing of deepfake pornography without consent has increased significantly in recent years. In 2019, Deeptrace found that the four largest deepfake porn websites had attracted 134,364,438 views.[12]

Women overwhelmingly appear as the objects of deepfake pornographic images and academic commentators 'have described the sharing of deepfake porn videos as a new means of degrading, humiliating, harassing and abusing women. Some women are particularly at risk. This includes female journalists, whose images are used in deepfake pornography to discredit, intimidate and silence them. Indeed, research indicates that the vast majority of those creating deepfake porn are men'.[13]

Academics have also noted that 'computer manipulation packages are so sophisticated that spotting fake images is not always easy", and it is likely that many altered images (such as those where a person's head is superimposed onto a body performing a sexual act) could be considered real and cause analogous harms to the person depicted as if it was an original photograph'.[14]

In 2018, the House of Commons' Women and Equalities Committee expressed support for criminalising the making of altered images without consent. In its report considering

[9] Ibid at 1, pg 164 - 165

[10] Law Commission (2021) Intimate Image Abuse A consultation paper, pg xi. Adopted from Danielle Citron and Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753.: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/02/Intimate-image-abuse-consultation-paper.pdf

[11] Ibid

[12] As cited at 10. Henry Ajder, Giorgio Patrini, Francesco Cavalli and another, "The State of Deepfakes: Landscape, Threats, and Impact" (September 2019) Sensity (formerly known as Deeptrace), available at https://sensity.ai/reports/ (last visited 23 February 2021).

[13] Ibid at 10, pg 211

[14] As cited at 10. Alisdair Gillespie, "'Trust me, it's only for me': 'revenge porn' and the criminal law" [2015] Criminal Law Review 866 at p 870

sexual harassment of women and girls in public places, it stated:

> *The Government should introduce a new law on image-based sexual abuse which criminalises all non-consensual creation and distribution of intimate sexual images, including altered images, and threats to do so.*[15]

The use of deepfake pornography in online Violence Against Women and Girls was debated in the House of Commons on 2nd December 2021. Introducing the motion, Maria Miller MP explained her reasons for bringing the debate:

> *Technology is being used every day to invent new and even more grotesque ways of inflicting abuse, particularly sexual violence, especially against women and girls. I have secured this debate on deepfake and nudification image abuse because they are yet more forms of abuse against women and girls, their impact is not understood, and they continue to be largely unrecognised, especially in law and the legal sanctions that are available.*
>
> *[…]At the moment, deepfakes are not against the law, and people who use nudification software are not recognised as sexually abusing others. Deepfakes have been a shocking development in violence against women online. Let us be clear: this technology is almost exclusively used to inflict violence against women. Indeed, the cyber research firm Sensity found that 96% of all deepfakes are pornographic and that all the pornographic deepfakes it detected—100%—targeted women.*
>
> *Offline, non-consensual sexual acts are recognised in the criminal law through the crimes of sexual assault, sexual abuse, rape—the list goes on, yet those responsible for developing and using technology in the online world and through artificial intelligence have been allowed to operate perniciously and with impunity, inflicting online sexual attacks on women and girls without criminal consequences.*
>
> *[…]Deepfakes are widely regarded by academics as the future of violence against women online, but the existing law is woefully behind and largely redundant. Section 33 of the Criminal Justice and Courts Act 2015, the so-called revenge porn legislation, in whose drafting I was involved, was a good step in the right direction, but it specifically excludes altered or photoshopped images and videos;*[16]

The criminalisation of revenge pornography in Northern Ireland was introduced by

[15] House of Commons Women and Equalities Committee Sexual harassment of women and girls in public places HC701: https://publications.parliament.uk/pa/cm201719/cmselect/cmwomeq/701/701.pdf

[16] HC Deb 2 December 2021: https://hansard.parliament.uk/Commons/2021-12-02/debates/F4FD1906-7A15-4F4E-B060-710C8EB26ADC/web

sections 51- 53 of Justice Act (Northern Ireland) 2016[17]:

**51**—(1) It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made—

(a)without the consent of an individual who appears in the photograph or film, and

(b)with the intention of causing that individual distress.

A person guilty of the offence is liable on conviction on indictment to imprisonment for a term not exceeding 2 years or a fine (or both). On summary conviction, the offence carries a maximum imprisonment term not exceeding 6 months or a fine not exceeding the statutory maximum (or both).

However, it is unclear whether deepfake revenge pornography would fall within the umbrella of this offence. For the purpose of the offence 'photographed or filmed images includes photographed or filmed images that have been altered in any way'. However, altered photographs do not necessarily meet the threshold of 'private' and 'sexual' to commit the offence:

A photograph or film is "private" if it shows something that is not of a kind ordinarily seen in public.

(3) A photograph or film is "sexual" if—

(a)it shows all or part of an individual's exposed genitals or pubic area,

(b)it shows something that a reasonable person would consider to be sexual because of its nature, or

(c)its content, taken as a whole, is such that a reasonable person would consider it to be sexual.

(4) Subsection (5) applies in the case of—

(a)a photograph or film that consists of or includes a photographed or filmed image that has been altered in any way,

(b)a photograph or film that combines two or more photographed or filmed images, and

(c)a photograph or film that combines a photographed or filmed image with something else.

[17] Justice Act (Northern Ireland) 2016: https://www.legislation.gov.uk/nia/2016/21/contents

(5) The photograph or film is not private and sexual if—

(a)it does not consist of or include a photographed or filmed image that is itself private and sexual,

(b)it is only private or sexual by virtue of the alteration or combination mentioned in subsection (4), or

(c)it is only by virtue of the alteration or combination mentioned in subsection (4) that the person mentioned in section 51(1)(a) and (b) is shown as part of, or with, whatever makes the photograph or film private and sexual.

Therefore, for example, 'a person who has non-consensually disclosed a private and sexual photograph of his or her former partner in order to cause that person distress will not be able to avoid liability for the offence by digitally changing the colour of the intended victim's hair. However, a person who simply transposes the head of a former partner onto a sexual photograph of another person will not commit the offence'.[18]

Images which are completely computer generated but made to look like a photograph or film are also not covered by the offence.

2.3 *Overlap with Existing Offences*

Depending on the nature and context of cyberflashing or deepfake pornography, they may constitute an offence under the following existing legislation:

- the Malicious Communications (NI) Order 1988 which makes it an offence to send indecent, offensive, threatening or false letters or articles with intent to cause distress or anxiety.[19] It attracts a penalty of a fine of up to £2,500.
- the Protection from Harassment (Northern Ireland) Order 1997 which prohibits the act of harassment. The maximum penalty on indictment conviction (heard in a crown court) is up to 2 years' imprisonment and/or a fine. On summary conviction (heard in a magistrates' court), the maximum penalty is 6 months' imprisonment. The Order also provides for the offence of 'putting people in fear of violence'. A person convicted of this offence on indictment conviction is liable to imprisonment for up to seven years, or a fine or both; or on summary conviction, to imprisonment for a term not exceeding six months, or a fine up to £5,000.[20]
- the Communications Act 2003 which makes it an offence to use public electronic

[18] CPS Guidance https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual

[19] Malicious Communications (NI) Order 1988,Article 3: https://www.legislation.gov.uk/nisi/1988/1849/article/3

[20] Protection from Harassment Order (NI) 1997, Article 3 and Article 6: https://www.legislation.gov.uk/nisi/1997/1180/contents

communications networks to send a message or any other matter that is grossly offensive or menacing and provides for a penalty of a maximum of six months' imprisonment and/or a fine of £5,000.[21]

- Offences under The Protection of Children (Northern Ireland) Order 1978 (where the image was taken before the subject turned 18).
- Unauthorised access to computer material under Section 1 of the Computer Misuse Act 1990 (where the images have been obtained through computer hacking).

[21] Communications Act 2003, Section 127: https://www.legislation.gov.uk/ukpga/2003/21/section/127

# 3 Internet Law and Regulation as a Reserved Matter

Schedule 2 of the Northern Ireland Act 1998 sets out those matters which are 'excepted', meaning the Northern Ireland Assembly cannot legislate in these areas. Schedule 3 sets out matters which are 'reserved', meaning the Assembly cannot legislate in these areas unless the Secretary of State for Northern Ireland lays before Parliament the draft of an Order in Council amending Schedule 3 so that the matter ceases to be reserved. The Secretary of State cannot make such an Order unless the Assembly has passed, with cross-community support, a resolution stating that it wishes the matter to cease to be reserved.[22]

Internet law and regulation is a reserved policy area under all three devolution settlements.[23] Therefore, any decision on telecommunication legislation is currently a matter for the UK Government. However, as noted by the Law Commission for England and Wales 'this is more relevant to the non-criminal law response to online harms, as acknowledged in the Government response to the Online Harms White Paper: "Devolution" paras 6.15 to 17.'[24].

The White Paper stated that:

> *Internet services and their regulation is a reserved issue, therefore the government intends for our proposed framework to apply on a UK wide basis". However, the government is conscious that some of the harms that will likely be in the scope and some aspects of enforcement involve devolved competences*.[25]

Clarifying the Devolution test in the Impact Assessment of the Online Harms Bill, the Department for Digital, Culture, Media and Sport stated that:

> *While some of the harms relate to offences in Scottish or Northern Irish Law, and therefore involve devolved competences, the legislation is not seeking to change the law in relation to these offences. Instead, our proposals seek to clarify the responsibility of businesses to tackle this activity on their services.[26]*

Justice and policing are transferred matters on which the Northern Ireland Assembly has full legislative powers, by virtue of the Northern Ireland Act 1998 (Amendment of

[22] Northern Ireland Act 1998, Section 4: https://www.legislation.gov.uk/ukpga/1998/47/section/4

[23] Northern Ireland Act 1998, Schedule 3: https://www.legislation.gov.uk/ukpga/1998/47/schedule/3

[24] Ibid at 1, pg 9

[25] Home Office and the Department for Digital, Culture, Media and Sport (2020), Online Harms White Paper: Full government response to the consultation, para 6.15: https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

[26] Home Office and the Department for Digital, Culture, Media and Sport (2021), The Online Safety Bill Impact Assessment: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf

Schedule 3) Order 2010.[27] Consequently, the Northern Ireland Executive does have significant scope to develop and implement policies relating to devolved matters and harms, for example, child abuse safety as a result of its devolved responsibility for education, policing and child protection. The law, therefore, addresses the abuse of children via the internet as well as elsewhere.

As the general position in law is that what is illegal offline is also illegal online, the Executive can keep various aspects of the criminal law under review and strengthen it where necessary. For example, when discussing the Protection from Stalking Bill, a Department of Justice official indicated that they thought it would be possible, under the bill, to secure a successful conviction based on exclusively online stalking behaviour:

> *I think that the answer should be yes. Essentially, you are looking for a pattern of behaviour, and what you describe would fit the criteria. I have been in contact with a number of victims who have been stalked largely online. In one case, the person lifted stuff from their online site and used it in their place of employment to suggest that the victim was a sex offender. They were working only online, but they were interfering with the person's online identity and putting out false and malicious statements about them online. That, clearly, is stalking behaviour and would certainly fit in to our definition without any problem*.[28]

[27] Northern Ireland Act 1998 (Amendment of Schedule 3) Order 2010: https://www.legislation.gov.uk/uksi/2010/977/contents/made

[28] NIA OR Committee for Justice, 21 January 2021:http://data.niassembly.gov.uk/HansardXml/committee-25076.pdf

# 4 UK Wide Developments

There have been growing calls 'for a coherent, unified body of law aimed specifically at online activities'.[29] Over the past number of years, the UK Government has considered how the internet can become a safer place for users, through the application of rules and online behaviour. It has done so using a dual approach looking at the regulation of platforms and the effectiveness of current legal provisions:

- The introduction of the Internet Safety Green Paper in 2017 and the Online Harms White Paper in 2019, which focused on the regulation of platforms, lead to the publication of a draft Online Harms Bill in May 2021;
- The Law Commission for England and Wales' projects in recent years have examined the criminal law provisions that apply to individuals and not the liability of platforms.

*Regulation of Online Harms*

An Online Harms White Paper was published in April 2019, which said that the existing 'patchwork of regulation and voluntary initiatives' had not gone far or fast enough to keep UK users safe.[30] Therefore, it proposed a single regulatory framework to tackle a range of online harms. At its core would be a new statutory duty of care for internet companies, including social media platforms. An independent regulator would oversee and enforce compliance with the duty. The White Paper received mixed reactions - although Children's charities were largely supportive, some commentators raised concerns that harms were inadequately defined. Others were concerned that the proposals could adversely impact on freedom of expression.[31]

Following the White Paper's publication, the Government undertook a 12-week public written consultation, alongside a programme of stakeholder engagement. An initial response to the consultation was published in February 2020. This stated, among other things, that the Government was minded to make Ofcom the regulator for online harms. A full response was published in December 2020. It confirmed that a duty of care would be introduced through an Online Safety Bill and that Ofcom would be the regulator. Again, reaction was mixed.

On 12 May 2021, the Government published the Online Safety Bill. All provisions of the Bill will apply to England, Wales, Scotland and Northern Ireland. In line with the Government's December 2020 response to its Online Harms consultation, the draft Bill would impose duties of care on providers of online content-sharing platforms and

[29] HC Library Briefing, 9 June 2017, Online harassment and cyber bullying

[30] HM Government, Online Harms White Paper, April 2019, p30: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf

[31] HC Library Briefing 28 May 2021, Regulating online harms: https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf

search services. Ofcom would enforce compliance and its powers would include being able to fine companies up to £18 million or 10% of annual global turnover, whichever is higher, and have the power to block access to sites.

Part 2 of the draft Bill sets out the duties of care that would apply to providers of user-to-user and search services. All regulated services would have to take action to tackle 'illegal content' and 'content that is harmful to children'. Category 1 regulated services[32] would also have to address "content that is harmful to adults".

The Government has stated:

> *In line with the government's response to the Online Harms White Paper, all companies in scope will have a duty of care towards their users so that what is unacceptable offline will also be unacceptable online.*
>
> *They will need to consider the risks their sites may pose to the youngest and most vulnerable people and act to protect children from inappropriate content and harmful activity.*
>
> *They will need to take robust action to tackle illegal abuse, including swift and effective action against hate crimes, harassment and threats directed at individuals and keep their promises to users about their standards.*
>
> *The largest and most popular social media sites (Category 1 services) will need to act on content that is lawful but still harmful such as abuse that falls below the threshold of a criminal offence, encouragement of self-harm and mis/disinformation. Category 1 platforms will need to state explicitly in their terms and conditions how they will address these legal harms and Ofcom will hold them to account.*
>
> *The draft Bill contains reserved powers for Ofcom to pursue criminal action against named senior managers whose companies do not comply with Ofcom's requests for information. These will be introduced if tech companies fail to live up to their new responsibilities. A review will take place at least two years after the new regulatory regime is fully operational*.[33]

The meaning of harmful content is set out in the lengthy clauses of 45 to 47 of the draft Bill. In summary, 'regulated content' would be considered harmful:

- if it is designated in secondary legislation as "primary priority content" that is harmful to children or "priority content" that is harmful to children or adults;
- if a service provider has "reasonable grounds to believe that the nature of the

[32] These are high risk and high reach platform providers such as Twitter and Facebook

[33] Gov.UK DCMS/Home Office Press Release 12 May 2021: https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities"; and

- if a service provider has "reasonable grounds to believe that there is a material risk" of the dissemination of the content "having a significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities".[34]

The Department for Digital, Culture, Media and Sport estimates a potential impact on the criminal justice system in the following areas. Namely, the introduction of:

- a new criminal offence for entities that fail to comply with information requests;
- a potential new criminal offence for named senior managers who fail to comply with information requests; and
- potential new criminal liability of corporate officers where an entity's failure to comply with an information request is committed with the consent or connivance of a director or senior official.[35]

A Joint Committee on the Draft Bill was established by the House of Lords and the House of Commons. The Committee reported its findings in December 2021.[36] It noted the negative impact of cyberflashing on recipients :

> *the unsolicited sending of images of genitalia is a particularly prevalent form of online VAWG.[…] Regardless of the intention(s) behind it, cyberfashing can violate, humiliate, and frighten victims, and limit women's participation in online spaces. The use of deepfake pornography in online VAWG is also becoming increasingly prevalent and is of great concern[…].*

The Committee recommended that:

> *The criminal law relating to online communication pre-dates the age of social media and modern search engines. It needs updating. We welcome the Law Commission's recommendations to reform this. We want to see new offences on the statute book at the first opportunity for harmful, threatening and knowingly false communications, cyberfashing […]*
>
> *We heard that the sending of unsolicited penis images was a particular problem for young women and girls, a concern borne out by the findings of Ofsted in its report on sexual abuse in schools. Research suggests such images are frequently not sent with intent to distress or for sexual gratification but that a*

[34] Draft Online Safety Bill, Clause 45-47: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

[35] Ibid at 26

[36] HL and HC Joint Committee on the Draft Online Safety Bill Report of Session 2021–22: https://publications.parliament.uk/pa/jt5802/jtselect/jtonlinesafety/129/129.pdf

> *"large amount of it is a kind of male bonding among their peers. That is why they share unsolicited nude images as well; they want to share among their peer group, 'Oh, we've sent them'."*

In relation to deepfake pornography, it said:

> *Knowingly false and threatening communications such as deepfake pornography should be made illegal and tech companies should be held responsible for reducing its spread.*[37]

*Law Commission for England and Wales*

The Law Commission for England and Wales has carried out two related projects on *Modernising Communications Offences* and *Intimate Image Abuse* which address the behaviour of cyberflashing and deepfake pornography. The Commission explained the overlap between the two projects as follows:

> *Offences that fall within the scope of intimate image abuse (where intimate images of a person are taken, made or shared without their consent) may well also fall within the scope of the harm-based communications offence that we recommend. However, some instances of intimate image abuse are sufficiently serious that the level of culpability cannot adequately be captured by a communications offence. Further, a conviction for a communications offence will not carry with it the range of possible ancillary orders (such as Sexual Harm Prevention Orders.*[38]

*Modernising Communications Offences* was a review of the criminal law governing harmful, threatening, and false communications, as well as encouraging and assisting serious self-harm, and cyberflashing. The review addressed the criminal law provisions that apply to individuals and not the liability of platforms. This project was funded by the Department for Digital, Culture, Media & Sport as part of the Government's Online Harms strategy. The Commission published a scoping report in November 2018, and a Consultation Paper followed in September 2020. It published its report and recommendations in July 2021. In the report, the Commission recommended the following new or reformed criminal offences:

1. **a new 'harm-based' communications offence** to replace the offences within section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988;
2. **a new offence of encouraging or assisting serious self-harm**;

[37] Ibid

[38] Ibid at 1, pg 8 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/07/Modernising-Communications-Offences-2021-Law-Com-No-399.pdf

3. **a new offence of cyberflashing**; and,
4. **new offences of sending knowingly false communications, threatening communications, and making hoax calls to the emergency services,** to replace section 127(2) of the Communications Act 2003.

The Law Commission specifically recommended that a new offence of cyberflashing be included in the Sexual Offences Act 2003 to address the 'harmful and increasing phenomenon' with the following elements[39]:

(1) The defendant (A) intentionally sent an image or video recording of any person's genitals to another person (B), and

(2) either- (a) A intended that B would see the image or video recording and be caused alarm, distress or humiliation, or (b) A sent the image or video recording for the purpose of obtaining sexual gratification and was reckless as to whether B would be caused alarm, distress or humiliation.

It found that its view that the current law is inadequate to combat cyberflashing 'was not challenged by any consultees. In particular, the Crown Prosecution Service agreed "that this area of law requires updating given the advances of technology".[40]

It considered that cyberflashing would be best addressed by a specific sexual offence of cyberflashing in addition to the exposure offence found in section 66 of the Sexual Offences Act 2003:

> *The evidence we have received of the harm caused by cyberflashing, as well as support from significant bodies within the criminal justice system, has fortified our view that cyberflashing – just as with its "offline" equivalent, exposure – should be classed as a sexual offence. This would not only label the offence fairly, but would also allow for the range of evidential and ancillary orders that this would permit (both at investigation, trial and conviction stages). For example, were cyberflashing listed in Schedule 3 of the Sexual Offences Act, then – pursuant to section 80 of the Sexual Offences Act 2003 – individuals convicted of cyberflashing could be subject to notification requirements (known colloquially as "being on the sex offenders' register"). While notification requirements are not automatically imposed as a result of being convicted of any offence under the Sexual Offences Act 2003, many of the sexual offences in that Act are included in Schedule 3 and sufficiently serious convictions of those offences do lead to notification requirements being automatically imposed. Doing so for this offence would assist the police with management of offenders within the community. Notably, the section 66 exposure offence appears in Schedule 3, and we see no*

[39] Ibid at 1, pg 193

[40] Ibid at 1, pg 170

*reason why cyberflashing ought not also to be included.*[41]

The proposed offence would be technologically neutral so 'it does not matter over or through what medium you send the image, nor should the offence be constrained to images of the sender's genitals. It is perhaps interesting to note in passing that the conduct element of the cyberflashing offence thus involves nothing inherently related to computer networks nor anything inherently related to public exposure'.

The Commission had originally proposed that cyberflashing should be addressed by amending section 66 of the Sexual Offences Act 2003 (exposure) to include the sending of images or video recordings of one's genitals. However:

> […]*with the benefit of evidence provided in consultation, we are now of the view that this solution is too narrow in scope and is susceptible to problems of proof. We recommend that it should be an offence for a person to send an image or video recording of genitals (whether the sender's or not) to another, either intending to cause that person alarm, distress or humiliation, or, where the image was sent for a sexual purpose, reckless as to whether it would cause alarm, distress or humiliation.*
>
> *We remain of the view that the offence should be a sexual offence, and specifically one that allows for ancillary orders such as Sexual Harm Prevention Orders and Notification requirements, colloquially known as requirements to sign the sexual offenders' register.*

The other project by the Law Commission, *Intimate Image Abuse,* reviews the existing criminal law as it relates to the taking, making and sharing intimate images without consent.[42] It ran a consultation on its proposals from February 2021 until May 2021. It is now analysing the responses to the consultation which will inform the development of its final recommendations for reform.

It identified that 'intimate image abuse is both wrongful and harmful. It is wrongful because it violates the victim's sexual privacy, autonomy and freedom, their bodily privacy and their dignity. A consequence of the wrongs of intimate image abuse is that it can cause victims to suffer serious and lasting harm'.[43] Upon analysing the issue of deepfake pornography, the Commission reached the view that:

> *sharing an altered intimate image without consent may cause serious harm and is a significant violation of the individual's bodily privacy, personal integrity and their dignity, and in some cases, their sexual privacy, autonomy and freedom. Therefore, we are of the view that this behaviour warrants criminalisation. We*

[41] Ibid at 1

[42] Ibid at 10

[43] Ibid at 10, p 14

> *provisionally propose that altered images be included as part of the sharing offence' under section 33(2) of the Criminal Justice and Courts Act 2015.*

The Commission noted that:

> *This exclusion was not discussed during debates in Parliament, but it can perhaps be explained by the mischief the offence was seeking to tackle. When introducing the offence in the House of Lords, Lord Faulks defined "revenge porn" in this way: "perpetrators post sexual images of former lovers after the breakdown of their relationships in order to hurt their victims". Baroness Brinton added: "Cyberstalking, cyberbullying, sexting and now revenge porn are all about abuse of power and spreading information widely on the net". It is clear, therefore, that the mischief the offence was designed to tackle is the sharing of images with others, often online, in order to distress the victim. Sharing the image with the victim without consent, it might have been thought, cannot cause the same harm as sharing the image widely online.*

The Commission also identified another deepfake situation that potentially warrants criminalisation:

> *The first situation is images that depict someone being sexually assaulted (either by the person who disclosed the image to the person in the image or someone else). As noted at paragraph 7.139 above, it is likely that Parliamentarians were of the view that disclosing an intimate image to the person in the image would not cause them distress, or at least not the same degree of distress that sharing the image with others could. However, where an image depicts someone being sexually assaulted it is clear that viewing or receiving that image would cause the person in the image significant distress. This is not caught by the current disclosure offence.*[44]

*England and Wales*

A Private Members' Bill was introduced by Angela Richardson MP in June 2021 to the House of Commons entitled the Unsolicited Explicit Images and Deepfake Pornography Bill.[45] It aims to create the offences of sending unsolicited explicit digital images and of producing digitally-altered images or videos in which an individual is depicted pornographically without their consent; and for connected purposes. Its second reading is intended for February 2022.

[44] Ibid at 10, pg 214

[45]Unsolicited Explicit Images and Deepfake Pornography Bill: https://bills.parliament.uk/bills/2921

# 5 Scotland

## *5.1 Cyberflashing*

In Scotland, Section 6 of the Sexual Offences (Scotland) Act 2009 makes provision for the offence of 'coercing a person into looking at a sexual image'[46]:

> Coercing a person into looking at a sexual image
>
> (1)If a person ("A") intentionally and for a purpose mentioned in subsection (2) causes another person ("B")—
>
> (a)without B consenting, and
>
> (b)without any reasonable belief that B consents,
>
> to look at a sexual image, then A commits an offence, to be known as the offence of coercing a person into looking at a sexual image.
>
> (2)The purposes are—
>
> (a)obtaining sexual gratification,
>
> (b)humiliating, distressing or alarming B.
>
> (3)For the purposes of subsection (1), a sexual image is an image (produced by whatever means and whether or not a moving image) of—
>
> (a)A engaging in a sexual activity or of a third person or imaginary person so engaging,(b)A's genitals or the genitals of a third person or imaginary person.

This is an offence for A to cause B to look at a sexual image (a still image or a film) without B's consent or any reasonable belief in B's consent, for the purpose of A's sexual gratification and/or the humiliation, alarm or distress of B. For example, causing another person to look could mean sending an offending picture message, or putting a pornographic film on a TV in B's presence.

Although the offence was not originally introduced to address cyberflashing, its provisions are sufficiently broad to address instances of cyberflashing. The offence is framed as a sexual offence. On summary conviction, the maximum penalty is 12 months' imprisonment or a fine not exceeding the statutory maximum (or both). On indictment conviction, the penalty is imprisonment for a term not exceeding 10 years or a fine (or both).

[46] Sexual Offences (Scotland) Act 2009, Section 6: https://www.legislation.gov.uk/asp/2009/9/section/6

Police Scotland is unable to provide a precise number of cyber flashing convictions because of the way in which data is recorded.[47]

50(1)(a) of the 2009 Act allows for an accused person to be convicted of an alternative crime, if "the jury are not satisfied that the accused committed the offence charged but are satisfied that the accused committed the alternative offence (or as the case may be one of the alternative offences)".

*5.2 Deepfake Pornography*

Altering images or producing deepfake pornographic material is not a specific offence and the production of such material in itself would probably not amount to a criminal offence. However, the distribution, publication or sale of such material, where it appears to depict a person who has not consented to such a depiction may amount to a criminal offence. Depending on the facts and circumstances, this may be capable of being charged under offences including section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 (non-consensual sharing of intimate images), section 38 of the Criminal Justice and Licensing (Scotland) Act 2010 (threatening or abusive behaviour) or section 127 of the Communications Act 2003 (misuse of a public electronic communications network).[48]

Section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 can address deepfake revenge pornography as it makes it an offence where a person 'discloses, or threatens to disclose, a photograph or film which shows, or appears to show, another person ("B") in an intimate situation.[49] In doing so, A intends to cause B fear, alarm or distress or A is reckless as to whether B will be caused fear, alarm or distress.

A person who commits this offence is liable on summary conviction, to 12 months or a fine not exceeding the statutory maximum (or both). On conviction on indictment, the maximum penalty is 5 years' imprisonment or a fine (or both).

[47] Recorded Crime in Scotland, 2019-2020: https://www.gov.scot/publications/recorded-crime-scotland-2019-2020/pages/21/

[48] S6W-00472 https://www.parliament.scot/chamber-and-committees/debates-and-questions/questions/2021/06/03/s6w00472?qry=deepfake

[49] Abusive Behaviour and Sexual Harm (Scotland) Act 2016, Section 2: https://www.legislation.gov.uk/asp/2016/22/section/2

# 6 Republic of Ireland

## *6.1 Deepfake Pornography*

In September 2016, the Law Reform Commission published its *Report on Harmful Communications and Digital Safety*.[50] It contained 32 recommendations for reform and included a draft Harmful Communications and Digital Safety Bill intended to implement these reforms.

The main recommendations related to changes in the criminal law were:

- reform of the existing offence of harassment, to ensure that it includes online activity such as posting fake social media profiles; and that there should be a separate offence of stalking, which is really an aggravated form of harassment; and
- reform of the existing offence of sending threatening and intimidating messages, to ensure that it fully captures the most serious types of online intimidation.

The Harassment, Harmful Communications and Related Offences Act 2020[51] originated as a Private Member's Bill, sponsored by Brendan Howlin T.D., which was influenced by the Law Reform Commission's Report. Following the publication of the Bill, the Minister for Justice agreed to work with Deputy Howlin to amend the provisions therein.[52] The content of the Act was strongly influenced by those who have lost their lives due to online abuse, in particular Nicole Fox, whose mother subsequently campaigned to strengthen the law in that area.[53] As a result the Act is also known as Coco's Law.

This Act created new offences dealing with the non-consensual distribution of intimate images which are broad enough to address deepfake pornography.

Section 2 provides for an offence of distributing, publishing or threatening to distribute or publish an intimate image without consent with intent to cause harm or being reckless as to whether harm is caused. This offence criminalises the distribution or publication of an intimate image without the consent of the person who is the subject of the image. The person who distributes or publishes the intimate image must have intended, or been reckless as to whether these acts would seriously interfere with the peace and privacy of the other person or cause the other person harm, alarm or distress. Threatening to distribute or publish such an intimate image is also an offence. The

[50] Law Reform Commission (2016) *Harmful Communications and Digital Safety* September: http://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf

[51] Harassment, Harmful Communications and Related Offences Act 2020: https://data.oireachtas.ie/ie/oireachtas/act/2020/32/eng/enacted/a3220.pdf

[52] Harassment, Harmful Communications and Related Offences Bill 2017,Explanatory Memorandum: https://data.oireachtas.ie/ie/oireachtas/bill/2017/63/eng/memo/b63a17d-memo.pdf

[53] Nicole Fox died by suicide at the age of 21 in 2018 after suffering three years of online bullying and harassment. At the time, there was no legislation available to address online bullying.

maximum penalty on indictment conviction is up to 7 years' imprisonment and/or an unlimited fine.

Section 3 provides for an offence of recording, distributing or publishing an intimate image without consent. This is a strict liability offence as there is no requirement to prove an intention to cause harm. It will be sufficient that the taking, recording or distribution of the intimate image seriously interfered with the other person's peace and privacy or caused them harm, alarm or distress. The maximum penalty for this offence on summary conviction is 12 months' imprisonment and/or a €5,000 fine.

Section 4 provides for an offence of distributing, publishing or sending a threatening or grossly offensive communication. This offence applies to any form of message or communication, both online or offline. It criminalises the once-off sending of a threatening or grossly offensive message where the person who is sending the message or communication intends to cause harm to the person who is the recipient of the message. This offence is intended to deal with the most harmful forms of messages and communications, both online and offline, where there is a clear intent to cause harm. The maximum penalties for this offence for conviction on indictment are 2 years' imprisonment and/or an unlimited fine.

The Act defines an 'intimate image', as any visual representation made by any means including any photographic, film, video or digital representation of:

- of the person's genitals, buttocks or anal region and, in the case of a female, her breasts;
- of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts;
- in which the person is nude; or
- in which the person is engaged in sexual activity.

The word 'representation' is used to ensure that where an image is altered or doctored to represent another individual (including his or her body parts), it still falls within the sphere of the offences.[54]

At Committee Stage, there was a proposal to amend the proposed section 2 provisions 'to add in there "or depicted as being engaged in sexual activity" because these things can be Photoshopped or tampered with or images that do not exist can be attributed to people'. However, the Minister for Justice, Helen McEntee T.D., clarified that:

> *The section that is proposed to be inserted covers that by mentioning "any... digital representation" so any type of altering of images where there is a different head on a different body or any type of amendment to what was a real image*

[54] Harassment, Harmful Communications and Related Offences Bill 2017, Explanatory Memorandum https://data.oireachtas.ie/ie/oireachtas/bill/2017/63/eng/memo/b63a17d-memo.pdf

*suggesting that it is somebody else. It is covered within the definitions section.*[55]

### *6.1 Cyberflashing*

Academic commentary appears to regard the offences under section 45 of the Criminal Law (Sexual Offences) Act 2017[56] as sufficiently broad to address cyberflashing. Following a number of judgments of the High Court which struck out offences relating to public indecency and exposure, this section replaced section 18 of the Criminal Law Amendment Act 1935 to provides for new offences to address two types of behaviour. The first is exposure of genitalia and the second is inappropriate sexual behaviour which may not involve actual exposure.[57]

Under this section it is an offence for a person who 'exposes his or her genitals intending to cause fear, distress or alarm' to another person. It is also an offence when a person 'intentionally engages in offensive conduct of a sexual nature'. Offensive conduct of a sexual nature 'means any behaviour of a sexual nature which, having regard to all the circumstances, is likely to cause fear, distress or alarm to any person who is, or might reasonably be expected to be, aware of any such behaviour'.[58]

A person found guilty of an offence under this section is liable on summary conviction, to a class D fine or 6 months' imprisonment, or both. Conviction on indictment, warrants a class C fine or imprisonment for a term not exceeding 2 years, or both.

[55] Harassment, Harmful Communications and Related Offences Bill 2017: Committee Stage, 1 December 2020:https://www.oireachtas.ie/en/debates/debate/select_committee_on_justice/2020-12-01/3/

[56] Criminal Law (Sexual Offences) Act 2017: https://www.irishstatutebook.ie/eli/2017/act/2/section/45/enacted/en/html

[57] Explanatory Memorandum: https://data.oireachtas.ie/ie/oireachtas/bill/2015/79/eng/memo/b7915s-memo.pdf

[58] Ibid at 56

# 7 New Zealand

## *7.1 Deepfake Pornography*

The Harmful Digital Communication Act 2015[59] (HDCA) aims to deter, prevent and mitigate the harm caused to victims by cyber bullying, harassment and intimidation. It was enacted following recommendations from the Law Commission's review of existing laws in 2012, which found that 1 in 10 New Zealanders had experienced a harmful digital communication at some stage in their lives.

Section 22 of the HDCA contains an offence of causing harm by posting "a digital communication". Harm is defined in section 4 as "serious emotional distress. The offence is punishable by up to 2 years' imprisonment or a maximum fine of $50,000 for individuals and a fine of up to $200,000 for companies. A criminal offence under the HDCA is subject to the same youth justice process that applies to other offences. Therefore it is not applied to children under the age of 14, but can be applied to young people aged 14-16 under the youth justice system.[60]

The Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Bill was introduced on 2 July 2020 and completed its first reading on 10 March 2021.[61] The Bill aims to amend the Harmful Digital Communications Act 2015 by inserting a new section 22A. The proposed section would make it an offence to post a digital communication that is an intimate visual recording knowing the subject of the recording did not consent to it being posted or being reckless whether the subject consented to it being posted. The Explanatory Note to the Bill states this new offence responds to a form of sexual exploitation, often referred to as 'revenge pornography'. It also recognises that "consent must be shown to be express, voluntary and informed.

The Justice Committee examined the Bill. A number of respondents to its enquiry of the Bill were concerned that the provisions do not recognise the threat of deepfake technology. However, the Committee did not make a recommendation to that effect:

> *The member in charge of this bill, Louisa Wall MP, also recommended the bill provide for intimate visual recordings that have been digitally altered or created. This would essentially treat synthetic intimate visual recordings as another type of intimate visual recording. Submissions highlighted that the harm caused by synthetic images is no different to the harm caused by intimate visual recordings that have not been altered and occur without the consent of the person who is the subject of the recording, as a form of image-based sexual abuse. We were*

[59] Harmful Digital Communications Act 2015: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html
[60] https://www.netsafe.org.nz/what-is-the-hdca/

[61] The Bill is a Member's Bill proposed by Louisa Wall MP.

*unable to agree to this recommendation*.[62]

However, following that, an individual Supplementary Order Paper amendment has been submitted for the Bill in order to extend the application of the new offence to cover intimate visual recordings that are created or altered to appear to show an individual.[63]

Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Bill Commentary

[62] https://www.parliament.nz/resource/en-NZ/SCR_115762/3173b2ed17a7f64df00f3a16e40d62868feb83e2

[63] House of Representatives, Supplementary Order Paper, 7 December 2021 https://legislation.govt.nz/sop/members/2021/0103/latest/096be8ed81b83957.pdf

# 8 Singapore

## *8.1 Cyberflashing*

Amendments to Singapore's Penal Code were introduced by the Criminal Law Reform Act and Protection from Harassment (Amendment) Act, which were passed in May 2019. As a result, a new offence of sexual exposure was introduced from January 2020 following concern with the advance in technology which had facilitated sexual offences such as voyeurism and the distribution of intimate images without consent. The Penal Code Review Committee had noted that existing offences which covered some forms of exposure did not capture sexual or malicious motives, nor did they capture the 'essence' of the wrongdoing and were not characterised as a 'sexual offence'[64]

The offence criminalises the non-consensual exposure of genitals, whether in person or on-line, such as sending unsolicited images of genitals over an electronic medium to another person.[65] The offence is committed where a person intentionally distributes to another an image of their or another's genitals, intending that the victim see the image and that the offender does so for the purpose of obtaining sexual gratification or of causing the victim humiliation, distress or alarm:

> *In terms of motive requirements, the offence is at least broader than only requiring proof of sexual gratification, though it remains limited. It precludes instances of cyberflashing which may be carried out for the purpose of status-building, humour, or as a 'prank' by other young people.*[66]

An image includes an image of either the perpetrator's genitals, or another person's, overcoming the evidential requirement to prove the image to be of the perpetrator's. In addition, the conduct of offence is one of distribution, rather than receipt; removing any requirement to prove that the victim received the image or viewed it. The offence carries a maximum penalty of one year's imprisonment. If the victim is under the age of 14, jail for up to 2 years is compulsory, and the offender will also be liable to be fined or caned.[67]

[64] Ibid at 3

[65] Singapore Penal Code Section 377BF: https://sso.agc.gov.sg/Act/PC1871#pr377BF-

[66] Ibid at 3

[67] Singapore Legal Advice: https://singaporelegaladvice.com/law-articles/cybersexual-crimes-singapore-penalties/

# 9 United States of America

## *9.1 Cyberflashing*

In 2019, Texas became the first US state to introduce a new, specific state law criminalising cyberflashing. The sponsors of the legislation noted that the original law 'addresses the physical act of indecent exposure, but is silent to the increasingly prevalent occurrence of individuals sending sexually explicit images to an individual without their consent'.[68]

Section 21.19 of the Penal Code of Texas addresses 'Unlawful Electronic Transmission of Sexually Explicit Visual Material'.[69] A person commits an offence if the person knowingly transmits by electronic means visual material depicting any person engaging in sexual conduct or with the person's intimate parts exposed; or covered genitals of a male person that are in a discernibly turgid state; and is unsolicited and sent without the express consent of the recipient. An offence under this section is held to be a Class C Misdemeanour. with a maximum penalty of a $500 fine. It has been considered that:

> *This broad provision means that not only are images of penises included, but also of other forms of sexual activity, as well as clothed penises. The distribution of the sexual images must have been made without the 'express consent of the recipient'. The mens rea is straightforward in requiring only intentional distribution without consent of the sexual image. There is, therefore, no specific motive requirement in this provision*.[70]

The wide definition of sexually explicit visual material means that this provision becomes, in effect, an offence of sending pornography without consent. It has been suggested that 'such a definition may give rise to challenges in terms of enforcement and debates regarding overcriminalisation'.[71]

## *9.2 Deepfake Pornography*

The Yale Cyber Leadership Forum[72] notes that 'some argue that defamation law can be an adequate avenue for pursuing cases of deepfake pornography', however it believes that 'defamation laws are insufficient both because they apply to too narrow a subset of image-based sexual abuse, and because they ignore the core issue of consent that is at

[68] Ibid at 3

[69] Texas Penal Code, Section 21.19: https://texas.public.law/statutes/tex._penal_code_section_21.19

[70] Ibid at 3

[71] Ibid

[72] The Forum is a collaboration between Yale Law School's Center for Global Legal Challenges and Yale's Jackson Institute for Global Affairs.It brings together various lawyers, technologists, entrepreneurs, policymakers, and academics to tackle the most pressing cyber challenges in an interdisciplinary environment.

stake with this form of abuse'. The Forum argues that:

> *Pursuing a defamation case against non-consensual deepfake pornography would mean arguing that pornographic content is damaging to women's reputations. But such an argument perpetuates the patriarchal notion that it is wrong for women to be expressly sexual. Furthermore, it ignores the core issue that is at stake with deepfake pornography, which is not whether or not it is "false" or defamatory in its depiction. The central issue is not the damage to a women's image by being depicted sexually; it is the violation of consent. Obviously, in our current society, women's reputations, careers, and lives are far too often damaged by expressions of sexuality — but even in an alternate universe where it would cause a woman no measurable harm, socially or professionally, for there to be a video of her engaging in sexual activity online, the production, sharing, and hosting of such a video without permission would be wrong as a violation of consent. In another situation, if someone makes a deepfake or otherwise posts a nonconsensual video of someone who does sex work, the defense could argue that because the woman's reputation already involves sexual activity, her reputation is not being defamed by another video of sexual activity. Such an argument — and thus pursuit under defamation as a whole — would be missing the actual point, which is the violation of consent.*
>
> *Deepfakes are yet another example of technology growing exponentially faster than our laws, leaving people already at greater risk of harm without legal protection. While some have assured that we can, in fact, find legal protection under defamation, using defamation protections for cases of non-consensual deepfake pornography perpetuates harmful underlying gender stereotypes, without providing adequate protection against image-based sexual abuse. Indeed, as we have seen, even the narrow issue of deepfake pornography alone is not addressed in any adequate way by defamation laws. The more prudent legal path would therefore be to address the core of the issue — a lack of consent — and treat non-consensual deepfake pornography as what it is: a sexual offense.*[73]

Legislation specifically targeting deepfakes has been introduced in several states, including Virginia, California, New York, Texas, and Georgia.

**Virginia's** legislation did not create a new crime for deepfake creation and distribution, but rather expanded its existing law on revenge porn and distribution to include deepfake material. It amended its disclosure offence in July 2019 to include deepfake pornography. It added to the offence:

> *For purposes of this subsection, "another person" includes a person whose image was used in creating, adapting, or modifying a videographic or still image*

[73] Yale Cyber Leadership Forum (2021) Deepfake Pornography: Beyond Defamation Law: https://cyber.forum.yale.edu/blog/2021/7/20/deepfake-pornography-beyond-defamation-law

*with the intent to depict an actual person and who is recognisable as an actual person by the person's face, likeness, or other distinguishing characteristic.* [74]

This amendment attracted a great deal of media attention and was hailed as one of the first to criminalise the sharing of deepfake pornography without consent. Those found guilty of the misdemeanour face up to a year in jail and a $2,500 fine.

Shortly after Virginia enacted its deepfake law, **Texas** passed a law that focused on deepfake election interference. Senate Bill 751 makes it a crime to generate and publish a video using artificial intelligence in order to affect the outcome of an election. The act of creating and sharing a deepfake video within 30 days of an election with the intent to "injure a candidate or influence the result of an election" is a Class A misdemeanor which faces up to six months in jail, fine up to $1,000.[75]

In October 2019, **California** followed both Virginia and Texas by passing two deepfake related laws; one to prohibit nonconsensual deepfake pornography, and the other to prohibit deepfakes used to impact the outcome of an upcoming election.[76]

Assembly Bill 602 allows Californian residents to sue if their image is used for sexually explicit content. The legislation allows victims to 'seek injunctive relief and recover reasonable attorney's fees and costs'.[77] The Bill provides 'that a depicted individual, as defined, has a cause of action against a person who either (1) creates and intentionally discloses sexually explicit material if the person knows or reasonably should have known the depicted individual did not consent to its creation or disclosure or (2) who intentionally discloses sexually explicit material that the person did not create if the person knows the depicted individual did not consent to its creation'.

Furthermore, Assembly Bill 730 makes it illegal to create or distribute videos, images, or audio of politicians doctored to resemble real footage within 60 days of an election.

On November 30, 2020, **New York's** Governor signed a unique law addressing synthetic or digitally manipulated media. The law has two main components:

- First, the law establishes a postmortem right of publicity to protect performers' likenesses, including digitally manipulated likenesses, from unauthorized commercial exploitation for 40 years after death. Professional actors and the Screen Actors Guild had pushed for this law for years to protect their likenesses from unauthorized postmortem use, especially as technology has advanced and actors have begun to appear in movies years after their deaths

[74] Code of Virginia https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/

[75] Senate Bill 751: https://legiscan.com/TX/text/SB751/id/2027638/Texas-2019-SB751-Enrolled.html

[76] The Guardian https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce

[77] Assembly Bill 602: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

- Second, the law bans non-consensual computer-generated pornography and highly realistic false images created by artificial intelligence (AI).[1] For the purposes of this offence:

> "depicted individual" means an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in a performance that was actually performed by the depicted individual but was subsequently altered to be in violation of this section.
>
> "digitization" means to realistically depict the nude body parts of another human being as the nude body parts of the depicted individual, computer-generated nude body parts as the nude body parts of the depicted individual or the depicted individual engaging in sexual conduct, as defined in subdivision ten of section 130.00 of the penal law, in which the depicted individual did not engage.[78]

If a victim is successful, a court may award injunctive relief, punitive damages, compensatory damages, and reasonable court costs and attorney's fees.

**Georgia** has also introduced a prohibition on nude or sexually explicit electronic transmissions. A person violates the Georgia Code Title 16. Crimes and Offenses section if they, knowing the content of a transmission or post, knowingly and without the consent of the depicted person:

> (1) Electronically transmits or posts, in one or more transmissions or posts, a photograph or video which depicts nudity or sexually explicit conduct of an adult, including a falsely created videographic or still image, when the transmission or post is harassment or causes financial loss to the depicted person and serves no legitimate purpose to the depicted person; or
>
> (2) Causes the electronic transmission or posting, in one or more transmissions or posts, of a photograph or video which depicts nudity or sexually explicit conduct of an adult, including a falsely created videographic or still image, when the transmission or post is harassment or causes financial loss to the depicted person and serves no legitimate purpose to the depicted person.[79]

Any person who violates the Code section shall be guilty of a misdemeanor of a high and aggravated nature. Upon a second or subsequent violation of te Code section, an offender can be found guilty of a felony and, upon conviction faces imprisonment of not less than one but not more than five years, a fine of not more than $100,000, or both.

[78] Article 5 Right of Privacy https://www.nysenate.gov/legislation/laws/CVR/52-C#:~:text=Section%2052%2DC%20Private%20right,explicit%20depiction%20of%20an%20individual

[79] Georgia Code Title 16. Crimes and Offenses § 16-11-90 https://codes.findlaw.com/ga/title-16-crimes-and-offenses/ga-code-sect-16-11-90.html

# 10 Australia

*10.1 Deepfake pornography*

In Australia, a number of states have included images which have been altered within their definition of the image for the purpose of revenge pornography. A spokesperson for the Australian Minister for Communications, Cyber Safety and the Arts has suggested that all of these offences are broad enough to include deepfake pornography.[80]

For example, in **New South Wales,** the Crimes Act 1900 was amended by the passing of the Crimes Amendment (intimate images) Act 2017, to criminalise revenge pornography.[81]

Section 91P of the Crimes Act 1900 makes it an offence punishable by up to 3 years' imprisonment and/or a fine of $11,000 for a person to intentionally record an intimate image of another person without that other person's consent, while knowing or being reckless to the fact that the other person did not consent.

Section 91Q prescribes the same maximum penalty for anyone who intentionally distributes an intimate image of another person without that other person's consent, while knowing or being reckless to the fact that the other person did not consent.

Section 91R also prescribes the same penalty for anyone who threatens to record or distribute an intimate image without consent, intending the other person to fear the threat would be carried out.

For the purpose of the Act, an 'intimate image' is defined as:

- A person's private parts, or a person engaged in a private act, or
- An image altered to appear to show a person's private parts, or
- The person engaged in a private act, where a reasonable person would expect to be afforded privacy.[82]

New South Wales courts are also empowered to issue rectification orders, which compel offenders "to take reasonable steps to recover, delete or destroy images taken or distributed without consent". Disobeying this order could see an additional two years' jail and a $5,500 fine issued.

In **Western Australia**, the Criminal Law Amendment (Intimate Images) Act 2019

[80] Ibid at 3

[81] Crimes Amendment (Intimate Images) Act 2017: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2017-029

[82] The Crimes Act 1900: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1900-040

[83]amended the Criminal Code to introduce offences of distributing an intimate image and threatening to distribute an intimate image of a person. An image means a still or moving image, in any form, that shows, in circumstances in which the person would reasonably expect to be afforded privacy;

- the person's genital area or anal area, whether bare or covered by underwear; or
- in the case of a female person, or transgender or intersex person identifying as female, the breasts of the person, whether bare or covered by underwear;
- or the person engaged in a private act.

It specifically includes an image, in any form, that has been created or altered to appear to show any of the aforementioned things.

Distribution of an intimate image carries a maximum penalty of imprisonment for 3 years. On summary conviction the penalty is imprisonment for 18 months and a fine of $18,000.

In February 2019, the **Queensland** government passed legislation criminalising the publication of 'revenge porn.' The Criminal Code (Non-Consensual Sharing of Intimate Images) Amendment Act 2019 amended the Criminal Code, creating three revenge porn offences consisting of the publication, without a person's consent, of intimate images or videos of the person, or making a threat to do so.[84]

A moving or still image is one that depicts:

- A person engaged in a sexual act;
- The genital or anal region when it is bare or covered only by underwear; or
- The bare breasts of a female; or
- An image that has been altered to appear to show any of the above.

It includes an image that 'has been digitally obscured'.

These offences on conviction carry a maximum term of imprisonment of three years.

[83]Criminal Law Amendment (Intimate Images) Act 2019: https://www.legislation.wa.gov.au/legislation/statutes.nsf/RedirectURL?OpenAgent&query=mrdoc_41760.pdf

[84] The Criminal Code (Non-Consensual Sharing of Intimate Images) Amendment Act 2019: https://www.legislation.qld.gov.au/view/pdf/asmade/act-2019-001