THE NEW WORLD'S PANDEMIC: SEXUAL EXPLOITATION IN THE DIGITAL AGE

ROCIO IGLESIAS GONZALEZ*

I. INTRODUCTION

Mary is a fifteen-year-old who is excited about starting her sophomore year of high school. Unbeknownst to Mary, George, a classmate whose romantic advances Mary had rejected, created a sexually explicit image generated by artificial intelligence, most commonly known as a deepfake, of Mary and started sending it to other classmates. Once Mary discovered the deepfaked pictures, she and her parents sought legal advice on available remedies. Unfortunately, Mary lives in Nevada, a state that has no legislation addressing the issue of nonconsensual sexually explicit deepfakes. Similarly, at the federal level, Mary has no course of action against her offender. From one moment to the next, Mary went from an excited teenager about to start the school year to a victim without remedy against her offender for the creation and distribution of nonconsensual sexually explicit deepfakes. Hundreds of other victims share Mary's experience, prominently women and girls.

This paper addresses legislators' attempts to regulate the creation and distribution of nonconsensual sexually explicit deepfakes. Part II provides background on why legislation regulating deepfakes is necessary.[1] Part III discusses the steps taken in the United States by analyzing the bills passed in the state of California and the proposed legislation by the federal government to regulate deepfakes.[2] Additionally, the section also discusses the efforts taken by the European Union, the South Korean government, and the United Kingdom's legislature to combat the proliferation of non-consensual sexually explicit

* *Juris Doctor*, 2025, St. Thomas University Benjamin L. Crump College of Law; B.A. Psychology, 2022, Florida International University. Thank you to my parents, Marely and Lazaro, for their infinite support and all of the sacrifices they made to help me become who I am today and achieve my career goals. Thank you to my partner, Jonathan, for always supporting me and celebrating my achievements like his own. Finally, thank you to *St. Thomas Law Review* for this incredible opportunity.

[1] *See infra* Part II (providing information regarding several victims of AI-generated nonconsensual porn).

[2] *See infra* Part III.

deepfakes.[3] Part IV proposes a solution to how legislators should frame a statute that properly vindicates victims of this form of sexual abuse.[4] Finally, Part V concludes that currently, there is no proper remedy available for victims of deepfakes and no proper punishment for their offenders.[5]

II. BACKGROUND

It is undeniable that artificial intelligence technology provides multiple advantages to society's everyday lives. However, just like any other technology, it is prone to misuse; more specifically, it has created a new category of crimes: nonconsensual sexually explicit deepfakes.[6] These types of deepfakes are images or videos that "often contain the face of an actual person on a naked or partially clothed body that is not their own and disproportionately targets women."[7] Over the past years, as artificial intelligence advances, the images have become more realistic, and their circulation is growing alarmingly. A study conducted in 2023 showed a fifty-four percent increase from 2022 in nonconsensual sexually explicit deepfakes across the internet, and more images were expected to be uploaded by the end of 2023.[8]

The sexually explicit deepfake crisis is particularly prominent in middle schools and high schools across the United States.[9] In New Jersey, several tenth-grade girls informed administrators that boys from the school had utilized artificial intelligence to create nude pictures of them and were spreading them around the school.[10] However, the school administration and district did little to help the victims.[11] Similarly, in Seattle, the school administration was informed of circulating deepfake images by two girls, one fourteen-year-old and a fifteen-year-old. However, the school failed to inform the authorities of the incident because it was unsure as to its reporting duties.[12] Ultimately, after

---

[3] *See id.*

[4] *See infra* Part IV.

[5] *See infra* Part V (summarizing the proposed solution to the lack of legislation regulating AI-generated porn).

[6] *See Combating Sexual Deepfakes*, MULTISTATE, https://www.multistate.ai/deepfakes-sexual (last visited Oct. 17, 2025).

[7] *Id.*

[8] *See* Matt Burgess, *Deepfake Porn Is Out of Control*, WIRED (Oct. 16, 2023, 7:00 AM), https://www.wired.com/story/deepfake-porn-is-out-of-control/.

[9] *See* Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in Schools*, THE N.Y. TIMES (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html ("Boys in several states have used widely available 'nudification' apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia.").

[10] *See id.*

[11] *See id.* ("Five months later, the Manis and other families say, the district has done little to publicly address the doctored images or update school policies to hinder exploitative A.I. use.").

[12] *See id.*

reporting the incident to Child Protective Services, the school district released a statement in which it explained that:

> [I]t had talked with students, families and the police as part of its investigation into the deepfakes[,] . . . provided support to students who were affected . . . [and] reported the "fake, artificial-intelligence-generated images to Child Protective Services out of an abundance of caution," noting that "per our legal team, we are not required to report fake images to the police."[13]

In California, however, school administrators took action by expelling five boys who had created deepfaked images of their classmates.[14]

The Federal Bureau of Investigation warned on March 29, 2024, that "child sexual abuse material (CSAM) created with content manipulation technologies, to include generative artificial intelligence (AI), is illegal." "Federal law prohibits the production, advertisement, transportation, distribution, receipt, sale, access with intent to view, and possession of any CSAM, including realistic computer-generated images."[15] However, as shown by how the middle school and high school incidents of non-consensual sexually explicit deepfakes were handled, it seems that the warning has little to no effect. Further, even though the FBI announced that it had arrested and convicted two people for creating and being in possession of child porn created through artificial intelligence, the door is left open for people to create non-consensual deepfake porn depicting adults without any repercussions.[16]

Perhaps the most notorious deepfake victim was the popular singer and songwriter Taylor Swift.[17] Taylor Swift's non-consensual sexually explicit deepfake started circulating on social media platforms such as X and Instagram.[18] As users reported the deepfake, X reacted fast as it "temporarily blocked searches of Swift's name."[19] However, Taylor Swift's case is distinct from other victims because Taylor Swift has the resources to pursue individual litigation—a recourse that many victims cannot afford to pursue.[20] Nonetheless,

---

[13] *Id.*

[14] *See id.*

[15] *Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal*, FBI (Mar. 29, 2024), https://www.ic3.gov/PSA/2024/PSA240329.

[16] *See id.* ("In November 2023, a child psychiatrist in Charlotte, North Carolina, was sentenced to 40 years in prison, followed by 30 years of supervised release, for sexual exploitation of a minor and using AI to create CSAM images of minors," and "[i]n November 2023, a federal jury convicted a Pittsburgh, Pennsylvania registered sex offender of possessing modified CSAM of child celebrities. The Pittsburgh man possessed pictures that digitally superimposed the faces of child actors onto nude bodies and bodies engaged in sex acts.").

[17] Brian Contreras, *Tougher AI Policies Could Protect Taylor Swift—And Everyone Else—From Deepfakes*, SCI. AM. (Feb. 8, 2024), https://www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/.

[18] *See id.*

[19] *Id.*

[20] *See id.*

Taylor Swift's deepfake incident has fast-tracked already in the works regulation of artificial intelligence.[21]

Adding to the issue is the fact that the biggest and most visited artificial intelligence-generated porn website is at the top of Google results when people search "deepfake porn."[22] Similarly, when users searched for a celebrity name followed by the word deepfake, Google's top results were the deepfake pornographic images featuring the celebrity.[23] Further,

> Googling "fake nudes" returned links to multiple apps and programs to create and view nonconsensual deepfake porn in the first six results, followed by six articles about high school boys' allegedly using the technology to create and share deepfake nude images of their female classmates. On Bing, searching "fake nudes" returned dozens of results of nonconsensual deepfake tools and websites before surfacing an article about the harms of the phenomenon.[24]

Even though Google representatives have stated that they will remove the pornographic deepfakes from the search results at the request of the victim, it does not proactively remove or block the deepfaked content.[25] Similarly, Microsoft's search engine, Bing, produces its own chatbot as a result, but it "tells users that it can't show them deepfake porn [because] [t]he use of deepfakes is unethical and can have serious consequences."[26] But just like Google, Bing does nothing to remove the links directing users to nonconsensual deepfake porn.[27]

The misuse of artificial intelligence can make anyone a victim of non-consensual deepfake porn, from celebrities to nonfamous adults and high schoolers. Artificial intelligence is growing alarmingly fast, making images more realistic, which could have a devastating impact on victims' lives. A film by Rosie Morris called My Blonde GF details "what happened to writer Helen Mort when she

---

[21] *See* Solcyré Burga, *How a New Bill Could Protect Against Deepfakes*, TIME (Jan. 31, 2024, 4:34 PM), https://time.com/6590711/deepfake-protection-federal-bill/ ("The federal bill, introduced on Tuesday, came nearly a week after deepfake pornographic images of Taylor Swift flooded X."); *see also* Leah Sarnoff, *Taylor Swift and No AI Fraud Act: How Congress Plans to Fight Back Against AI Deepfakes*, ABC NEWS (Jan. 30, 2024, 11:36 AM), https://abcnews.go.com/US/taylor-swift-ai-fraud-act-congress-plans-fight/story?id=106765709 ("Rep. Morelle said he hopes the abuse against Swift will be a driving force in getting the No AI FRAUD Act established.").

[22] *See* Kat Tenbarge, *Found Through Google, Bought With Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 11:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 ("A Google search for 'deepfake porn' returned MrDeepFakes as the first result.").

[23] *See* Kat Tenbarge, *Google and Bing Put Nonconsensual Deepfake Porn at the Top of Some Search Results*, NBC NEWS (Jan. 11, 2024, 9:10 AM), https://www.nbcnews.com/tech/internet/google-bing-deepfake-porn-image-celebrity-rcna130445.

[24] *Id.*

[25] *See id.*

[26] *Id.*

[27] *See id.* ("But dozens of links to and examples of nonconsensual deepfake porn are a click away on Bing.").

found out photos of her face had appeared on deepfake images on a porn site."[28] Helen Mort ("Mort") explains in the film that it "feels as if 'people on the street somehow knew about the pictures, and they knew this horrible secret about me, which suddenly felt like my horrible secret.'"[29] Mort further explained that she "did feel as if those were real images."[30] In the film, Mort also details the "un-imaginable worry of not knowing who created the images" and how "police were unable to do anything to prosecute whoever had made the images."[31]

Noelle Martin ("Martin"), an eighteen-year-old law student, recounted her experience as "completely horrifying, dehumanizing, degrading, violating to just see yourself being misrepresented and being misappropriated in that way."[32] Martin expressed that "being a victim of image-based abuse changed the trajectory of her life" because "'[i]t robs you of opportunities, and it robs you of your career, and your hopes and your dreams,' . . . 'it's been extremely hard for [her] to find employment.'"[33] She tried to contact "the police, private investigators, and government agencies, but because she didn't know where the images originated, there was no way to hold the creators accountable."[34] At one point, "Martin even attempted to contact the operators of the porn sites that hosted the pornographic photos of her, but those efforts sometimes led to more abuse."[35] Currently, Martin dedicates herself to speaking out about this kind of sexual abuse; however, due to this, she is now the target of perpetrators even more.[36]

Non-consensual, sexually explicit deepfakes are the new form of sexual abuse and are going unchecked. Legislators are struggling with how to regulate artificial intelligence technology, and it is mainly taking them so long to create policies because they themselves do not fully understand how it operates. In the meantime, however, millions of victims are being targeted and sexually abused by having their faces plastered on pornographic videos. At the same time, the perpetrators and social media and technology companies are not being held accountable or punished, and if they are, what they receive is a slap on the wrist at most. With no real legal consequences, victims are left helpless, the perpetrators free, and the tech companies go about their day making millions of dollars.

---

[28] Helen Bushby, *Deepfake Porn Documentary Explores Its 'Life-Shattering' Impac*t, BBC (June 17, 2023), https://www.bbc.com/news/entertainment-arts-65854112.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Justin Sherman, *"Completely Horrifying, Dehumanizing, Degrading": One Woman's Fight Against Deepfake Porn*, CBS NEWS (Oct. 14, 2021, 7:00 AM), https://www.cbsnews.com/news/deepfake-porn-woman-fights-online-abuse-cbsn-originals/.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

III. DISCUSSION

A. CALIFORNIA'S ATTEMPTS TO REGULATE NON-CONSENSUAL SEXUALLY EXPLICIT DEEPFAKES

Concerned with the proliferation of sexually explicit deepfakes, California became the second state to pass legislation targeting the issue.[37] In 2019, Assembly Bill No. 602 created a cause of action "against a person who intentionally distributes a photograph or recorded image of another that exposes the intimate body parts of that person or of a person engaged in a sexual act without the person's consent if specified conditions are met."[38] The bill was later codified into Section 1708.86 of the California Civil Code.[39] In the subsequent years, the California legislature introduced eight additional bills addressing sexually explicit deepfakes; however, only three were approved by the legislators and signed by Governor Newsom.[40]

The first bill, SB-981, was passed by both the California Assembly and Senate and signed into law by Governor Newsom on September 19, 2024.[41] SB-981 "would require a social media platform to provide a mechanism that is reasonably accessible to a reporting user who is a California resident who has an account with the social media platform to report sexually explicit digital identity theft to the social media platform."[42] The Senate Bill would also require social media platforms "to immediately remove a reported instance of sexually explicit digital identity theft from being publicly viewable on the social media platform if the social media platform determines there is a reasonable basis to believe the reported sexually explicit digital identity theft is sexually explicit digital identity theft."[43] The material covered under the bill includes:

> (A) The material is an image or video created or altered through digitization that would appear to a reasonable person to be an image or video of any of the following:
>
> (i) An intimate body part of an identifiable person.
>
> (ii) An identifiable person engaged in an act of sexual intercourse,

---

[37] *See Combating Sexual Deepfakes*, *supra* note 6; *With AI, anyone can be a victim of nonconsensual porn. Can laws keep up?*, 19TH NEWS (Mar. 11, 2024, 6:00 AM), https://19thnews.org/2024/03/ai-deepfakes-legislation/ ("Governing bodies are trying to catch up. In the past year or so, 10 states have passed legislation to criminalize the creation or dissemination of deepfakes specifically.").

[38] *See* Assemb. B. 602 § 1708.86, 2019–2020 Leg., Reg. Sess. (Cal. 2019).

[39] CA CIV. CODE § 1708.86 (2023).

[40] *See Combating Sexual Deepfakes*, *supra* note 6 (tracking AI legislation in 2024 targeted to combat sexual deepfakes); *Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, GOV. GAVIN NEWSOM (Sept. 19, 2024), https://www.gov.ca.gov/2024/09/19/governor-newsom-signs-bills-to-crack-down-on-sexually-explicit-deepfakes-require-ai-watermarking/.

[41] *See Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, *supra* note 40.

[42] S.B. 981, 2023–2024 Leg., Reg. Sess. (Cal. 2024).

[43] *Id.*

sodomy, oral copulation, or sexual penetration.

(iii) An identifiable person engaged in masturbation.

(B) The reporting person is the person depicted in the material, and the reporting person did not consent to the use of the reporting person's likeness in the material.

(C) The material is displayed, stored, or hosted on the social media platform.[44]

The reasoning behind the bill was explained by Dr. Aisha Wahab, who stated that victims of deepfakes, who are not celebrities, do not have the ability "to have the internet scrubbed of digitized sexually explicit media in less than 24 hours."[45] Thus, according to Dr. Wahab, "[t]he digital divide is as much about power on the internet as it is about access to it, and SB 981 will rebalance that power by requiring platforms to be more proactive when they receive reports of sexually explicit digital identity theft."[46] SB-981 would be added as Chapter 22.7 (commencing with Section 22670) to Division 8 of the Business and Professions Code relating to social media platforms.[47] The bill will go into effect on January 1, 2025.[48]

The second bill, SB-926, passed the last week of August 2024, would:

[M]ake it a crime for a person who is 18 years of age or older to intentionally create and distribute or cause to be distributed any photo-realistic image, digital image, electronic image, computer image, computer-generated image, or other pictorial representation of an intimate body part or parts of another identifiable person, or an image of the person depicted engaged in the act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates that was created in a manner that would cause a reasonable person to believe the image is an authentic image of the person depicted, under circumstances in which the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress.[49]

Dr. Wahab, who introduced the bill, explained that "victims of digital sexual assault are forever traumatized by their perpetrators through damaged reputations that lead to a lack of workplace promotions, mental health deterioration,

---

[44] *Id.*

[45] *Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, *supra* note 40.

[46] *Id.*

[47] *See* S.B. 981 § 22671(b)(1).

[48] *See September 24, 2024: Governor Gavin Newsom Signs Groundbreaking LADA-Sponsored AI Porn Bills Into Law*, L.A. DIST. ATT'Y'S OFF. (Sept. 24, 2024), https://da.lacounty.gov/media/news/governor-gavin-newsom-signs-groundbreaking-lada-sponsored-ai-porn-bills-law.

[49] S.B. 926, 2023–2024 Leg., Reg. Sess. (Cal. 2024).

shame, and isolation[.]"[50] Therefore, "SB 926 gives these victims—who are predominantly women—and law enforcement the tools they need to ensure perpetrators are prosecuted to the full extent of the law."[51] The bill was signed into law by Governor Newsom on September 19, 2024, and it would go into effect on January 1, 2025, as an amendment to 647 of the California Penal Code.[52]

The last bill, AB-1831, which passed the Assembly and the Senate on August 31, 2024, amends child pornography laws to include content that was digitally altered or created by the use of artificial intelligence.[53] AB-1831 is significant because "[c]urrent law does not allow district attorneys to go after people who possess or distribute [artificial intelligence]-generated child sexual abuse images if they cannot prove the materials are depicting a real person."[54] Governor Newsom signed the bill into law on September 29, 2024.[55] In a statement, Marc Berman, who introduced the bill, expressed the following:

> I'm grateful to Governor Newsom for signing AB 1831, which will ensure that the sexual exploitation of children in California is illegal—including [artificial intelligence]-generated pictures and videos of children being sexually abused. This would not be possible without the powerful advocacy from survivors of [artificial intelligence]-generated sexual exploitation, like Disney star Kaylin Hayman, who bravely testified to the lasting harm this digital abuse causes to children. I'm grateful to law enforcement for bringing this to my attention and working with me to make sure more children aren't victimized in the future.[56]

The regulation of sexually explicit deepfakes is crucial, as there have been countless incidents involving nonconsensual sexually explicit deepfakes.[57]

---

[50] *Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, *supra* note 40.

[51] *Id.*

[52] *See Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, *supra* note 40; *see also September 24, 2024: Governor Gavin Newsom Signs Groundbreaking LADA-Sponsored AI Porn Bills Into Law*, *supra* note 48.

[53] Assemb. B. 1831, 2023–2024 Leg, Reg. Sess. (Cal. 2024).

[54] Trân Nguyễn, *California Lawmakers Approve Legislation to Ban Deepfakes, Protect Workers and Regulate AI*, AP NEWS (Sept. 1, 2024, 3:06 AM), https://apnews.com/article/california-ai-election-deepfakes-safety-regulations-eb6bbc80e346744dbb250f931ebca9f3#.

[55] *Governor Newsom Announces New Initiatives to Advance Safe and Responsible AI, Protect Californians*, GOV. GAVIN NEWSOM (Sept. 29, 2024), https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians/.

[56] *California Criminalizes AI-Enabled Child Sexual Abuse*, MARC BERMAN ASSEMBLYMEMBER, DIST. 23 (Sept. 29, 2024), https://a23.asmdc.org/press-releases/20240929-california-criminalizes-ai-enabled-child-sexual-abuse.

[57] *See* Kylar Harris & Artemis Moshtaghian, *High Schooler Calls for AI Regulations After Manipulated Pornographic Images of Her and Others Shared Online*, CNN (Nov. 4, 2023, 7:26 PM), https://edition.cnn.com/2023/11/04/us/new-jersey-high-school-deepfake-porn/ (explaining how at least thirty female high school students were victims of AI-generated pornography); Kat Tenbarge & Liz Kreutz, *A Beverly Hills Middle School is Investigating Students Sharing AI-made Nude Photos of Classmates*, NBC NEWS (Feb. 27, 2024, 6:10 PM),

California is recognizing the growing dangers of artificial intelligence, and its legislators are doing a great job at regulating it. Artificial intelligence regulation in the state of California is particularly important because "[t]he state is home to 32 of the world's 50 leading [artificial intelligence] companies, high-impact research and education institutions, and a quarter of the technology's patents and conference papers."[58] In another pioneering act, just in August, the San Francisco City Attorney "announced a first-of-its-kind lawsuit today against some of the world's largest websites that create and distribute non-consensual [artificial intelligence]-generated pornography."[59]

There is no question that the new legislation will provide new and additional avenues to vindicate victims of nonconsensual artificial intelligence-generated pornographic images. However, there is still more work to do. Los Angeles County District Attorney George Gascón ("District Attorney Gascón") expressed "that the new penalties for sharing [artificial intelligence]-generated revenge porn should have included those under 18, too."[60] Former District Attorney Gascón is correct in his assertion since there have been a significant amount of incidents where the perpetrators are minors targeting their classmates.[61]

Even though regulation could be stricter, it is important to recognize that California is taking significant steps in combating the creation of non-consensual sexually explicit artificial intelligence images. Other states that already have deepfake legislation in place should follow California's steps and enact stricter laws to further benefit the victims, punish perpetrators, and hold social media companies accountable. At the same time, states that have not enacted any type of legislation addressing non-consensual sexually explicit deepfakes should look at California's new policies as a guide.

---

https://www.nbcnews.com/tech/misinformation/beverly-vista-hills-middle-school-ai-images-deepfakes-rcna140775 ("Students at a middle school in Beverly Hills, California, used artificial intelligence technology to create fake nude photos of their classmates, according to school administrators."); *see* Clare Duffy, *Have You Been Targeted by Non-consensual Deepfake Pornography?*, CNN (July 25, 2024, 7:00 AM), https://www.cnn.com/2024/07/25/tech/non-consensual-deepfake-pornography-callout/index.html ("Women around the world, from Taylor Swift and Rep. Alexandria Ocasio-Cortez to high school girls in New Jersey and Texas, have been targeted by non-consensual, AI-generated sexual images in recent months.").

[58] *Governor Newsom Announces New Initiatives to Advance Safe and Responsible AI, Protect Californians*, *supra* note 55.

[59] *City Attorney Sues Most-Visited Websites That Create Nonconsensual Deepfake Pornography*, CITY ATT'Y OF S. F. (Aug. 15, 2024), https://www.sfcityattorney.org/2024/08/15/city-attorney-sues-most-visited-websites-that-create-nonconsensual-deepfake-pornography/; *see The US Needs Deepfake Porn Laws. These States Are Leading the Way*, WIRED (Sept. 5, 2024, 6:00 AM) https://www.wired.com/story/deepfake-ai-porn-laws/ ("Last month, San Francisco City Attorney David Chiu's office announced a lawsuit against 16 of the most visited websites that allow users to create AI-generated pornography.").

[60] Trân Nguyễn, *California Governor Signs Bills to Protect Children from AI Deepfake Nudes*, AP NEWS (Sept. 29, 2024, 8:40 PM), https://apnews.com/article/ai-deepfakes-children-abuse-7dcf5c566e2a297567f1e148ac2074a4.

[61] *See* Singer, *supra* note 9.

B. CONGRESS' ATTEMPTS AT ENACTING LEGISLATION TO REGULATE NON-CONSENSUAL SEXUALLY EXPLICIT DEEPFAKES

Although currently, there are forty-eight states with laws criminalizing revenge porn, with deepfakes emerging as a new form of sexual abuse, not many states are keeping up—and certainly not the federal government.[62] The biggest problem with criminalizing the creation, distribution, and consumption of non-consensual sexually explicit deepfakes is the lack of federal regulation.[63] Fortunately, the problem might be solved soon.

The first federal efforts to try regulating deepfakes were seen in 2018 when House Representative Yvette Clarke (D-N.Y.) and Senator Ben Sasse (R-Neb.) attempted to introduce different bills that would criminalize deepfakes, but the bills were short-lived.[64] In September 2023, House Representative Yvette Clarke reintroduced the "DeepFakes Accountability Act," establishing criminal penalties and providing legal recourse to deepfake victims.[65] The bill, however, has not gotten anywhere. In May 2023, "Rep. Joe Morelle (D-N.Y.) introduced the Preventing Deepfakes of Intimate Images Act, which would have criminalized the sharing of non-consensual and sexually explicit deepfakes."[66] But just like other attempts to regulate deepfakes, the bill died shortly after being introduced.[67]

Early in 2024, the first attempts to tackle the issue of non-consensual sexually explicit deepfakes were seen. Before the Taylor Swift deepfake began circulating social media platforms, on January 10, Republican Representative Maria Elvira Salazar, with the support of other bipartisan U.S. House lawmakers, had introduced the "No Artificial Intelligence Fake Replicas And Unauthorized Duplications (No AI FRAUD) Act of 2024."[68] No AI FRAUD aims to establish a federal framework for protecting one's voice and likeness while establishing clear First Amendment protections.[69] Although No AI FRAUD is

---

[62] *See* Mariel Padilla, *With AI, Anyone Can Be a Victim of Nonconsensual Porn. Can Laws Keep Up?*, 19TH NEWS (Mar. 11, 2024, 6:00 AM), https://19thnews.org/2024/03/ai-deepfakes-legislation/ (explaining that the legislation regarding deepfakes at the state and federal level and "[i]n 2023, more than 143,000 new AI-generated videos were posted online, according to The Associated Press").

[63] *See id.* ("The biggest gap is that the U.S. doesn't have federal law.").

[64] *See* Lorena O'Neil, *Fake Photos, Real Harm: AOC and the Fight Against AI Porn*, ROLLINGSTONE (Apr. 8, 2024, 10:00 AM), https://www.rollingstone.com/culture/culture-features/aoc-deepfake-ai-porn-personal-experience-defiance-act-1234998491/.

[65] *See* H.R. 5586, 118th Cong. (2024).

[66] O'Neil, *supra* note 64.

[67] *See* H.R. 3106, 118th Cong. (2024).

[68] *See* H.R. 6943, 118th Cong. (2024).

[69] *See Salazar Introduces the No AI Fraud Act*, CONGRESSWOMAN MARIA ELVIRA SALAZAR FLA.'S 27TH DIST. (Jan. 10, 2024), https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act; *see also* Kristin Robinson, *House Lawmakers Unveil No AI FRAUD Act in Push for Federal Protections for Voice, Likeness*, BILLBOARD (Jan. 10, 2024), https://www.billboard.com/business/legal/no-ai-fraud-act-congress-federal-law-explained-1235578930/.

primarily constructed to protect the intellectual property of artists, after Taylor Swift became a victim of deepfake porn, Maria Elvira Salazar expressed that:

> "What happened to Taylor Swift is a clear example of [artificial intelligence] abuse. My bill, the No AI FRAUD Act, will punish bad actors using generative [artificial intelligence] to hurt others — celebrity or not," . . . . "Everyone should be entitled to their own image and voice and my bill seeks to protect that right."[70]

After being introduced, however, the No AI FRAUD Act has not received further action despite receiving widespread support from music business executives from different companies such as Sony, Universal Music Group, The American Society of Composers, Authors and Publishers, the Recording Industry Association of America, the Recording Academy, the National Music Publishers' Association, SoundExchange, the American Association of Independent Music, and Latin Recording Academy.[71] Opponents of the bill have explained that the content covered under the bill is too broad and could include "pictures of your kid, to recordings of political events, to docudramas, parodies, political cartoons, and more."[72] Second, opponents express concern because the No AI FRAUD Act creates a new intellectual property right; thus, "Section 230 immunity does not apply to federal IP claims, so performers (and anyone else who falls under the statute) will have free rein to sue anyone that hosts or transmits [artificial intelligence]-generated content."[73] Third, opponents criticize the statute of limitations on using deceased people's voices or likenesses.[74] Lastly, opponents state that the balancing test between the First Amendment and intellectual property rights that courts would apply under the No AI FRAUD Act is too strict.[75] Although the No AI FRAUD Act has not passed either the U.S. House of Representatives or the U.S. Senate, one of the other bills introduced is gaining widespread support in Congress from both Democrats and Republicans.

Recently, House Representative Alexandria Ocasio-Cortez—a victim herself of non-consensual sexually explicit deepfakes—introduced in the House a bill called "Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act" of 2024.[76] On the Senate side, the bill is sponsored by Senator Dick Durbin and Senator Lindsey Graham.[77] The DEFIANCE Act would not be a new law; instead, it would amend the Violence Against Women Act,

---

[70] Sarnoff, *supra* note 21.
[71] *See* Robinson, *supra* note 69.
[72] Corynne McSherry, *The No AI Fraud Act Creates Far More Problems Than It Solves*, ELEC. FRONTIER FOUND. (Jan. 19, 2024), https://www.eff.org/deeplinks/2024/01/no-ai-fraud-act-creates-way-more-problems-it-solves.
[73] *Id.*
[74] *See id.*
[75] *See id.*
[76] *See* O'Neil, *supra* note 64 (explaining how House Representative Alexandria Ocasio-Cortez was a victim of sexually explicit deepfakes and what led her to introduce the House version of the DEFIANCE Act).
[77] *See id.*

which protects survivors of sexual assault and domestic violence.[78] The Act's purpose is to provide deepfake victims with a federal cause of action in civil court against those who create, distribute, possess, or solicit non-consensual porn generated by artificial intelligence.[79] The victims would be entitled to damages up to $150,000 or $250,000 "if the conduct at issue [] was committed in relation to actual or attempted sexual assault, stalking, or harassment of the identifiable individual by the defendant; or the direct and proximate cause of actual or attempted sexual assault, stalking, or harassment of the identifiable individual by any person."[80] Additionally, the victims could recover attorney's fees and litigation fees.[81] The DEFIANCE Act passed in the Senate in July 2024 and is currently waiting for a vote in the House of Representatives.[82]

While the DEFIANCE Act would provide a civil remedy for deepfake victims, several other congressmen are attempting to criminalize non-consensual sexually explicit deepfakes. On May 23, 2024, Senator Maggie Hassan, a Democrat, and Senator John Cornyn, a Republican, introduced the "Preventing Deepfakes of Intimate Images Act."[83] The Act would amend Section 1309 of the Violence Against Women Act Reauthorization Act of 2022, and it would "create a new criminal offense for sharing these images, along with a 'private right of action' for victims to file a lawsuit against parties—including websites—that intentionally share the images."[84] The criminal penalties under the Act include up to two years in prison or up to ten years in prison if:

> [T]he violation in which the disclosure or threatened disclosure of the covered digital depiction could be reasonably expected to—
>
> (i) affect the conduct of any administrative, legislative, or judicial proceeding of a Federal, State, local, or Tribal government agency, including the administration of an election or the conduct of foreign relations; or
>
> (ii) facilitate violence.[85]

---

[78] *See* Mohar Chatterjee, *Nonconsensual AI Porn is Hated on the Left and Right. Can Congress Act on it?*, POLITICO (May 26, 2024, 12:00 PM), https://www.politico.com/news/2024/05/26/ai-deepfake-porn-congress-00158713 ("Rather than write a new law, Durbin's office crafted an amendment to the Violence Against Women Act that protects survivors of sexual assault and domestic violence.").

[79] *See* S.B. 3696, 118th Cong. (2024).

[80] *Id.*

[81] *See id.*

[82] *See id.*; *see also* Kat Tenbarge, *The Defiance Act Passes in the Senate, Potentially Allowing Deepfake Victims to Sue Over Nonconsensual Images*, NBC NEWS (July 24, 2024, 3:28 PM), https://www.nbcnews.com/tech/tech-news/defiance-act-passes-senate-allow-deepfake-victims-sue-rcna163464 ("A federal bill that would allow victims of nonconsensual sexually explicit deepfakes to sue people who create, share and receive them has unanimously passed the Senate and now moves to the House for a vote.").

[83] S.B. 4409, 118th Cong. (2024).

[84] Miranda Nazzaro, *Bipartisan Senators Introduce Bill to Fight Nonconsensual 'Deepfake Porn*,*'* THE HILL (May 23, 2024, 5:15 PM), https://thehill.com/homenews/senate/4682884-deepfake-porn-senate-bill/; *see* S.B. 4409.

[85] S.B. 4409.

The civil penalties, on the other hand, include the actual damages sustained by the victim, $150,000 in liquidated damages, or punitive damages.[86]

A month after the Preventing Deepfakes of Intimate Images Act was introduced, another bipartisan bill was presented. Concerned with the fact that up to 95% of all internet deepfake videos depict non-consensual intimate imagery, Senator Ted Cruz ("Senator Cruz") and other senators introduced "The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Network (TAKE IT DOWN) Act."[87] The bipartisan bill would criminalize the publication or threat to publish non-consensual intimate imagery or revenge porn in interstate commerce.[88] Additionally, the TAKE IT DOWN Act provides that:

> Social media and other websites would be required to have in place procedures to remove [non-consensual intimate imagery], pursuant to a valid request from a victim, within 48 hours. Websites must also make reasonable efforts to remove copies of the images. The FTC is charged with enforcement of this section.[89]

On the other hand, the TAKE IT DOWN Act would protect "the good faith disclosure of [non-consensual intimate imagery], such as to law enforcement or for medical treatment" and lawful speech.[90] Like the DEFIANCE Act, the TAKE IT DOWN Act would not create a separate law but instead, amend Section 223 of the Communications Act of 1934.[91] Senator Cruz requested unanimous consent to pass the legislation; however, his efforts were blocked by Senator Cory Booker—no other senator objected.[92]

All of the bills introduced in both the U.S. Senate and the U.S. House of Representatives demonstrate that Congress believes sexually explicit deepfakes are a significant problem in the country. Moreover, all of the bills introduced have been bipartisan efforts and have drawn bipartisan support, which demonstrates that both Democrats and Republicans, at least, agree that legislation

---

[86] *See id.*

[87] *See* S.B. 4569, 118th Cong. (2024); *see also Sen. Cruz Leads Colleagues in Unveiling Landmark Bill to Protect Victims of Deepfake Revenge Porn*, U.S. SENATE COMM. ON COM., SCI. & TRANSP. (June 18, 2024), https://www.commerce.senate.gov/2024/6/sen-cruz-leads-colleagues-in-unveiling-landmark-bill-to-protect-victims-of-deepfake-revenge-porn ("Up to 95 percent of all internet deepfake videos depict [non-consensual intimate imagery], with the vast majority targeting women and girls.").

[88] *The TAKE IT DOWN Act*, TODD YOUNG U.S. SEN. FOR IND., https://www.young.senate.gov/wp-content/uploads/1-pager_TAKE-IT-DOWN-Act_6.18.2024-FINAL.pdf (last visited Oct. 17, 2025).

[89] *Id.*

[90] *Id.*

[91] *See* S.B. 4569; *see also* Chatterjee, *supra* note 78 (explaining that the DEFIANCE ACT is a proposed amendment to the Violence Against Women Act).

[92] *See Sen. Cruz's Bipartisan Effort to Protect Teenagers from Deepfake 'Revenge Porn' Blocked by Sen. Booker*, U.S. SENATE COMM. ON COM., SCI. AND TRANSP. (Sept. 26, 2024), https://www.commerce.senate.gov/2024/9/sen-cruz-s-bipartisan-effort-to-protect-teenagers-from-deepfake-revenge-porn-blocked-by-sen-booker.

regulating non-consensual porn created through the use of artificial intelligence is needed. Further, the legislators also agree that giving victims a voice is important, as shown by the creation of civil remedies in the DEFIANCE Act and the Preventing Deepfakes of Intimate Images Act, as well as by the provision regarding social media platforms in the TAKE IT DOWN Act.

Although the DEFIANCE Act, the TAKE IT DOWN Act, and the Preventing Deepfakes of Intimate Images Act are all steps in the right direction, more comprehensive legislation must be introduced. A comprehensive bill would include the federal civil remedy from the DEFIANCE Act and the Preventing Deepfakes of Intimate Images Act, with the criminal penalties that the Preventing Deepfakes of Intimate Images Act would create, plus the requirement that social media platforms remove non-consensual sexually explicit deepfakes as proposed by the TAKE IT DOWN Act. Legislation that punishes those engaged in the creation, distribution, and consumption of non-consensual porn created by artificial intelligence, holds social media platforms accountable, and protects victims is necessary to fully address the problem that deepfakes pose to society.

C. STEPS TAKEN BY THE EUROPEAN UNION TO REGULATE NON-CONSENSUAL SEXUALLY EXPLICIT DEEPFAKES

On August 1, 2024, the European Union's AI Act came into effect; the Act is the first piece of legislation in the world to regulate artificial intelligent systems.[93] The AI Act creates a "uniform framework across all [European Union] countries, based on a forward-looking definition of [artificial intelligence] and a risk-based approach."[94] The risk classifications are as follows:

> **Minimal risk:** most AI systems, such as spam filters and AI-enabled video games, face no obligation under the AI Act, but companies can voluntarily adopt additional codes of conduct.
>
> **Specific transparency risk**: systems like chatbots must clearly inform users that they are interacting with a machine, while certain AI-generated content must be [labeled] as such.
>
> **High risk:** high-risk AI systems such as AI-based medical software or AI systems used for recruitment must comply with strict requirements, including risk-mitigation systems, high-quality of data sets, clear user information, human oversight, etc.
>
> **Unacceptable risk:** for example, AI systems that allow "social scoring" by governments or companies are considered a clear threat to people's fundamental rights and are therefore banned.[95]

---

[93] *See AI Act Enters Into Force*, EUR. COMM'N (Aug. 1, 2024), https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.
[94] *Id.*
[95] *Id.*

Regarding deepfakes, the European Union's AI Act "[doesn't] ban them entirely, . . . and instead decided to require that [artificial intelligence] creators act generally in a manner that is transparent. According to this framework, anyone who creates or uses a deepfake must disclose its artificial origin and provide information about the techniques that are used."[96] Deepfakes fall under the specific transparency risks.[97] The placement of deepfakes under the specific transparency risk "is certainly debatable in consideration of the harm they are capable of causing, [however], the good news is that the AI Act also provides the theoretical possibility that deepfakes could fall into the 'high-risk category' due to the potential for manipulation of political or electoral content."[98] Unfortunately, the AI Act makes no specific reference to the regulation of spreading non-consensual sexually explicit deepfakes.

The AI Act approach to deepfakes focuses on the principle of disclosure as a form of protection.[99] However, disclosure rules do not mitigate the harm caused by being a victim of deepfakes, such as depression, anxiety, or PTSD.[100] Further, "[d]isclosure alone does not tackle the deep-seated psychological, reputational and educational harms that children face when deepfakes are used as a form of gender-based violence or peer-to-peer bullying."[101] Therefore, the AI Act has two main gaps because the complexity of "deepfake technologies is underestimated" and "[d]isclosure and transparency are inadequate measures to overcome the potential psychological, mental and well-being impacts of deepfakes."[102]

Currently, victims of deepfakes in Europe "have to rely on a patchwork of laws like the EU's privacy bill, the General Data Protection Regulation (GDPR), and national laws on defamation."[103] Further, social media platforms "must make it easier for people and police to report potentially illegal content — and swiftly . . . take it down when it's the case — as part of the EU's content-moderation rulebook, the Digital Services Act (DSA)."[104] There are no laws, however, criminalizing non-consensual sexually explicit deepfakes.

Fortunately, earlier this year, the European Parliament and European Council agreed to criminalize deepfakes.[105] The agreement focuses on "domestic

---

[96] Jacobacci Avvocati, *AI and Deepfakes: EU and Italian Regulations*, LEGAL500, https://www.legal500.com/guides/hot-topic/ai-and-deepfakes-eu-and-italian-regulations/ (last visited Oct. 17, 2025).
[97] *See id.*
[98] *Id.*
[99] Nomisha Kurian, *EU AI Act: How Well Does it Protect Children and Young People?*, UNIV. OF CAMBRIDGE (Apr. 22, 2024), https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people.
[100] *See id.*
[101] *Id.*
[102] *Id.*
[103] Clothilde Goujard, *Taylor Swift Deepfakes Nudge EU to Get Real About AI*, POLITICO (Feb. 6, 2024, 6:44 PM), https://www.politico.eu/article/europe-eye-fix-taylor-swift-nude-deepfake/.
[104] *Id.*
[105] *See* Lisa Marie Segarra, *EU to Criminalize Non-Consensual Explicit Deepfakes*, PETAPIXEL

violence and violence against women, both online and offline," with a big emphasis on cyber violence, which includes "the non-consensual sharing of intimate images (including deepfakes), cyber-stalking, cyber-harassment, misogynous hate speech and 'cyber-flashing.'"[106] The European Commission Vice President has expressed that deepfakes are "[t]he latest disgusting way of humiliating women . . . . Such pictures can do huge harm, not only to popstars but to every woman who would have to prove at work or at home that it was a deepfake."[107] Regrettably, the law is not keeping up with the fast-growing technology facilitating the creation of deepfakes since it would not go into effect until mid-2027.[108]

Nonetheless, the European Union is also addressing deepfakes in the context of minors. On February 5, 2024, the European Commission adopted a proposal updating "the criminal law rules on child sexual abuse and child exploitation."[109] One key aspect of the proposal is to expand the definition of the criminal offenses related to child sexual abuse across the countries that are members of the European Union.[110] The rules update the definitions to now include as a crime "child sexual abuse material in [deepfakes] or AI-generated material."[111] The proposal would update the European Union's current rules, which date back to 2011.[112] The commissioner for home affairs explained that "[f]ast evolving technologies are creating new possibilities for child sexual abuse online, and raises challenges for law enforcement to investigate this extremely serious and wide spread crime[.]"[113]

Regarding deepfakes, the AI Act is less comprehensive than all the deepfake-related bills passed in California and all the proposed legislation by the United States Congress. Regulation in the United States focuses more on criminal penalties and a civil cause of action for victims to sue their perpetrators in addition to disclosure guidelines. Nonetheless, the European Union's AI Act is a pivotal piece of legislation in the right direction to regulating artificial intelligence. However, even though it is important to recognize the European Union's efforts to keep up with emerging and fast-growing technologies such as generative artificial intelligence, regulation is not being adopted fast enough, and it is not comprehensive enough. In the meantime, more women and girls suffer at the hands of their perpetrators by having their reputations and mental health

---

(Feb. 7, 2024), https://petapixel.com/2024/02/07/eu-to-criminalize-non-consensual-explicit-deepfakes/.

[106] *Id.*

[107] Goujard, *supra* note 103.

[108] *See id.*

[109] *The Fight Against Child Sexual Abuse Receives New Impetus With Updated Criminal Law Rules*, EUR. COMM'N (Feb. 5, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_631.

[110] *See id.*

[111] *Id.*

[112] Natasha Lomas, *EU Proposes Criminalizing AI-generated Child Sexual Abuse and Deepfakes*, TECHCRUNCH (Feb. 6, 2024, 10:57 AM), https://techcrunch.com/2024/02/06/eu-csa-deepfakes/.

[113] *Id.*

ruined due to the sexually explicit images created through the misuse of artificial intelligence.

D. THE SOUTH KOREAN DEEPFAKES PRACTICE AND THE STEPS TAKEN TO CRIMINALIZE DEEPFAKES

South Korea is facing a non-consensual deepfake porn crisis. According to a 2023 report on deepfakes globally by Security Hero, a United States startup focused on identity theft protection, "South Korea is the country most targeted by deepfake pornography, with its singers and actresses constituting 53% of the individuals featured in such deepfakes[.]"[114] In the first seven months of 2024, a total of 297 deepfake crimes were reported, "which is up from 180 in the whole of [2023] and 160 in 2021."[115] The crisis is primarily affecting minors, and the perpetrators are mostly teenagers, being responsible for committing two-thirds of the offenses over the past three years.[116] Over 200 schools are believed to have been affected by deepfake incidents, with a rise in targeting teachers.[117] The deepfakes are mainly shared through the social media application Telegram.[118] One of the most popular Telegram chatrooms, with the main purpose of creating and sharing deepfakes, has approximately 220,000 members.[119]

Women's rights activists have criticized the South Korean government, expressing that they do not believe that the current government, "which dismisses structural gender discrimination as mere 'personal disputes,' can effectively address [the deepfake] issues[.]"[120] Former President Yoon denied that women suffered from systemic gender discrimination "despite evidence to the contrary."[121] Further, "women hold just 5.8% of the executive positions in South Korea's publicly listed companies, and are paid on average a third less than South Korean men - giving the country the worst gender pay gap of any rich

---

[114] Reuters, *South Korea Police Launch Probe Into Whether Telegram Abets Online Sex Crimes, Yonhap Reports*, U.S. NEWS (Sept. 1, 2024), https://www.usnews.com/news/world/articles/2024-09-01/south-korea-police-launch-probe-into-telegram-over-online-sex-crimes-yonhap-reports.

[115] Jean Mackensie & Nick Marsh, *South Korea Faces Deepfake Porn 'Emergency*,*'* BBC (Aug. 28, 2024), https://www.bbc.com/news/articles/cg4yerrg451o.

[116] *See id.*; Social Media, *South Korea Confronts Deepfake Pornography Crisis as Digital Sex Crimes Surge*, ASEAN NOW (Aug. 28, 2024), https://aseannow.com/topic/1336686-south-korea-confronts-deepfake-pornography-crisis-as-digital-sex-crimes-surge/ ("Of the 178 individuals charged in these cases, 113 were teenagers, highlighting the disturbing involvement of youth in both the creation and distribution of these harmful images.").

[117] *See* Mackensie & Marsh, *supra* note 115.

[118] *See* Social Media, *supra* note 116.

[119] *See id.* ("One of the most notorious examples of the deepfake crisis involves a popular Telegram chatroom with approximately 220,000 members. This chatroom has become a hub for the creation and sharing of deepfake images, which are often made by doctoring photographs of women and girls.").

[120] Mackensie & Marsh, *supra* note 115.

[121] *Id.*

nation in the world."[122] In addition, South Korea's minister position for the Ministry of Gender Equality and Family has remained vacant since February 2024 "and the ministry's budget for preventing violence against women and aiding victims experienced a significant cut this year."[123] Even more, "[i]n a recently announced budget proposal for next year, the fund assigned to the Advocacy Center for Online Sexual Abuse Victims, which deletes online sexual abuse material, decreased from the previous year, despite the center's surging workload."[124] Therefore, women are reluctant to believe that the government can appropriately handle the current and ongoing deepfake crisis, where they are the main targets, and men are the offenders.[125]

However, the South Korean government has taken some measures in order to handle the situation. First, the South Korean authorities announced a crackdown on sexually abusive deepfakes.[126] They started an investigation into Telegram for aiding and abetting in spreading the deepfakes on the platform.[127] The investigation comes after Telegram's founder was arrested and indicted in France, in August, for alleged illegal activity on the application that includes "complicity in the distribution of child abuse images, drug trafficking and failure to comply with law enforcement requests."[128] Telegram has responded by apologizing to the authorities "for its handling of deepfake pornographic material shared via its messaging app, amid a digital sex crime epidemic in the country."[129] Further, Telegram's spokesperson has stated that the social media platform is "actively removing content reported from Korea that breached its terms of service and will continue to do so."[130] According to South Korea's Communications Standards Commission, Telegram confirmed that it had taken down twenty-five deepfake videos and proposed "an email address dedicated to future communication with the regulator."[131] The South Korean Communications Standards Commission, also expressed that Telegram's approach has been

---

[122] *Id.*

[123] Se Eun Gong, *South Korea investigates Telegram Over Alleged Sexual Deepfakes*, NPR (Sept. 6, 2024, 1:21 PM), https://www.npr.org/2024/09/06/nx-s1-5101891/south-korea-deepfake.

[124] *Id.*

[125] *See id.* ("[W]omen's rights groups said the 'root cause' of recurring digital sexual abuses is sexism. They blamed President Yoon Suk Yeol's government for failing to recognize that and letting the problem grow.").

[126] *See id.*

[127] *See id.*

[128] Stephanie Sy & Azhar Merchant, *Charges Against Telegram CEO Sparks Debate Over Balance of Free Speech and Responsibility*, PBS NEWS (Aug. 29, 2024, 6:25 PM), https://www.pbs.org/newshour/show/charges-against-telegram-ceo-sparks-debate-over-balance-of-free-speech-and-responsibility.

[129] Kelly Ng, *Telegram Apologises for Handling of Deepfake Porn Material*, BBC (Sept. 4, 2024), https://www.bbc.com/news/articles/cvg45kz47dno.amp.

[130] Gong, *supra* note 123.

[131] Ng, *supra* note 129.

"very forward-looking" and that the company has "'acknowledged the seriousness' of the situation."[132]

This is not the first time that Telegram has been involved in sexual abuses perpetrated against women. In 2020, the app was used to operate an online blackmail ring.[133] Although "[t]he leader of the ring, Cho Ju-bin, was sentenced to 42 years in prison for his role in blackmailing at least 74 women, including 16 teenagers, into sending degrading and sometimes violent sexual imagery of themselves[,]"[134] Telegram did not cooperate with the police "in preventing digital exploitation and in ensuring that those responsible were held accountable."[135] Therefore not much should be expected from Telegram in addressing the current deepfake crisis in South Korea, despite its pledge "to enforce a zero-tolerance policy on illegal deepfake content."[136]

In terms of law, South Korea "currently criminalizes doctored or fake materials that 'may cause sexual desire or shame' and are created 'for the purpose of dissemination[.]'"[137] Under the law, "those found guilty of creating sexually explicit deepfakes can be jailed for up to five years and fined up to 50 million won ($37,500; £28,300)."[138] However, "perpetrators often evade punishment."[139] Police statistics show that "[t]he arrest rate for fake sexual materials last year was 48%, far lower than the rate for other forms of digital sexual assault[.]"[140] Additionally, even if the perpetrators are tried, "about half of them get suspended sentences."[141] A review of court rulings revealed that:

> less than a third of the 87 people indicted by prosecutors for deepfake crimes since 2021 were sent to prison[,] [n]early 60 percent avoided jail by receiving suspended terms, fines or not-guilty verdicts, . . . and that [j]udges tended to lighten sentences when those convicted repented for their crimes or were [first-time] offenders.[142]

In a turn of events, in October, a South Korean court sentenced two men for spreading non-consensual sexually explicit images of women who attended South Korea's top university, Seoul National University, between 2021 and April 2024.[143] The two men created and distributed approximately 2,000

---

[132] *Id.*
[133] *See* Social Media, *supra* note 116.
[134] *Id.*
[135] Chyung Eun-ju & Joel Cho, *Telegram Deepfake Scandal Sparks Outrage, But Big Tech Stays Indifferent*, THE KOREAN TIMES (Sept. 3, 2024), https://www.koreatimes.co.kr/www/opinion/2024/09/197_381528.html.
[136] Hyung-Jin Kim, *In South Korea, Rise of Explicit Deepfakes Wrecks Women's Lives and Deepens Gender Divide*, PBS NEWS (Oct. 3, 2024, 6:55 PM), https://www.pbs.org/newshour/world/in-south-korea-rise-of-explicit-deepfakes-wrecks-womens-lives-and-deepens-gender-divide.
[137] Gong, *supra* note 123.
[138] Ng, *supra* note 129.
[139] Gong, *supra* note 123.
[140] *Id.*
[141] *Id.*
[142] Kim, *supra* note 136.
[143] *See* AFP, *South Korean Court Jails Man for 10 Years over Deepfake Porn*, FMT (Oct. 30, 2024,

degrading sexually explicit images generated by artificial intelligence "of women who attended the same alma mater as the men, Seoul National University."[144] One of the perpetrators, surnamed Park, was sentenced to ten years in prison, while the other offender, surnamed Kang, was sentenced to four years in prison.[145] Park's ten-year sentence is "the most severe penalty that has been handed down" under the current South Korean law criminalizing deepfakes.[146] Although the men asked for leniency due to—supposed—mental health struggles, the court was not persuaded and gave the following remarks:

> "The victims lived in fear and anxiety, suspecting all male acquaintances until the defendants were apprehended," . . . they also had to "live in constant unease and the recovery from their trauma (was) nearly impossible[.]" [T]he men's "actions were a twisted manifestation of inferiority and hatred toward socially successful women[,]" fuelled by the anonymity that Telegram provides.[147]

Although Park's and Kang's sentences brought justice to their victims, those sentences are outliers, and tougher laws are still needed. During the last week of September, South Korean lawmakers passed a bill criminalizing possessing or watching sexually explicit deepfake pictures and videos.[148] The new law states that "[a]nyone purchasing, saving or watching such material could face up to three years in jail or be fined up to 30 million won ($22,600)[.]"[149] Additionally, the new law increases the prison sentence for those creating sexual deepfakes from five years to seven.[150] Another deviation from current law is that under the new bill, the perpetrator does not need to have the intent to distribute in order to be jailed for the creation of deepfakes.[151] The bill is now waiting for the approval of President Yoon Suk Yeol in order to be enacted.[152]

Despite the new bill taking a firmer stance against deepfakes than the previous law, "South Korea still lags far behind other developed nations when it comes to laws against sexual violence."[153] For example, under the country's

---

9:00 PM), https://www.freemalaysiatoday.com/category/world/2024/10/30/south-korean-court-jails-man-for-10-years-over-deepfake-porn/.

[144] *Id.*

[145] *See id.*

[146] *Id.*

[147] *Id.*

[148] *See* Reuters, *South Korea to Criminalize Watching or Possessing Sexually Explicit Deepfakes*, CNN (Sept. 26, 2024, 11:31 PM), https://www.cnn.com/2024/09/26/asia/south-korea-deepfake-bill-passed-intl-hnk/index.html.

[149] *Id.*

[150] *See id.*

[151] *See* Emmet Lyons, *South Korea Set to Criminalize Possessing or Watching Sexually Explicit Deepfake Videos*, CBS NEWS (Sept. 27, 2024, 10:46 AM), https://www.cbsnews.com/news/south-korea-deepfake-porn-law-ban-sexually-explicit-video-images/.

[152] *See* Reuters, *supra* note 148.

[153] Jiwon Kim, *South Korean Women Have Another Digital Sex Crime to Worry About: Deepfake Porn*, THE DIPLOMAT (Oct. 25, 2024), https://thediplomat.com/2024/10/south-korean-women-have-another-digital-sex-crime-to-worry-about-deepfake-porn/.

"current regulations, rape is a matter of physical violence rather than that of consent."[154] In January 2023, "the Ministry of Gender Equality and Family submitted a proposal . . . to expand the legal definition of rape to 'non-consensual sexual activity,' to meet the international standard set by the United Nations framework on sexual violence[;] but it was quickly shot down by the administration."[155] Because "there is a deep divide between the genders in Korean society today[,]"[156] there is little hope that even the new law will bring justice to victims and put perpetrators in jail, especially because the majority of offenders are teenagers who are tried in youth court where sentences are more lenient.[157]

In the meantime, South Korean victims have spoken out about intense suffering.[158] In a letter, an unidentified victim explained that she had tried committing suicide because she did not want to suffer any longer from the deepfake videos made of her.[159] Another woman explained, "that her doctoral studies in the United States were disrupted for a year [and that] [s]he is receiving treatment after being diagnosed with panic disorder and post-traumatic stress disorder in 2022."[160] One of Park's and Kang's victims stated that "[b]uilding trust with men is stressful, . . . because she worries that 'normal-looking people could do such things behind my back.'"[161] A seventeen-year-old high schooler expressed that she feels scared of living as a woman in South Korea and that she feels awkward when talking with male friends and tries to distance herself from boys she does not know well.[162]

E. DEEPFAKE REGULATION IN THE UNITED KINGDOM

In 2023, the United Kingdom parliament passed the Online Safety Act of 2023 (the "Act"). The Act's purpose is to protect children and adults online.[163] There are several criminal offenses introduced under the Act that took effect on January 31, 2024.[164] The offenses include encouraging or assisting serious self-harm, cyber flashing, sending false information intended to cause non-trivial harm, threatening communications, intimate image abuse, and epilepsy trolling.[165] Further, the Act requires that platforms: implement measures to

---

154 *Id.*
155 *Id.*
156 *Id.*
157 *See* Jean Mackenzie & Leehyun Choi, *Inside the Deepfake Porn Crisis Engulfing Korean Schools*, BBC (Sept. 2, 2024), https://www.bbc.com/news/articles/cpdlpj9zn9go.
158 *See* Kim, *supra* note 136.
159 *See id.*
160 *Id.*
161 *Id.*
162 *See id.*
163 *See Online Safety Act: Explainer*, GOV.UK (May 8, 2024), https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer.
164 *See id.*
165 *See id.*

reduce the risks of their services being used for illegal offenses, put in place systems for removing illegal content when it does appear, and for search services to take steps to reduce the risks of users encountering illegal content via their services.[166] Additionally, "[p]latforms must also remove any other illegal content where there is an individual victim (actual or intended), where it is flagged to them by users, or they become aware of it through any other means."[167] The illegal content that the app covers includes child sexual abuse, controlling or coercive behavior, extreme sexual violence, extreme pornography, fraud, racially or religiously aggravated public order offenses, inciting violence, illegal immigration and people smuggling, promoting or facilitating suicide, intimate image abuse, selling illegal drugs or weapons, sexual exploitation, and terrorism.[168]

The sharing of intimate images is a priority offense under the Act.[169] Earlier this year, the United Kingdom government announced a proposal for a new law criminalizing the creation of sexually explicit deepfakes.[170] The new offense would be an amendment to the new Criminal Justice Bill, which would build on the existing offense under the Act.[171] "Under the new offen[s]e, individuals creating or designing intimate images of another person 'using computer graphics or any other digital technology' for the purposes of causing alarm, distress or humiliation to the person may face a criminal record and an unlimited fine under the new offen[s]e."[172] Perpetrators do not need to have the intent to share the deepfakes to be punished under the new offense, but if they do then they can also be charged "under the offen[s]e for sharing an intimate image and may face up to 2 years imprisonment."[173] The new law "will apply to images of adults, because the law already covers this [behavior] where the image is of a child."[174] On May 24, 2024, however, it was announced that the Criminal Justice Bill "including the proposal to create a new offen[s]e for making sexually explicit deepfakes[] will not be progressing further in its passage through Parliament[.]"[175]

---

166 *See id.*
167 *Id.*
168 *See id.*
169 *See* Paul Scully et al., *Government Crackdown on Image-Based Abuse*, GOV.UK (June 27, 2023), https://www.gov.uk/government/news/government-crackdown-on-image-based-abuse; *see also Criminalising Deepfakes – the UK's New Offences Following the Online Safety Act*, HERBERT SMITH FREEHILLS (May 21, 2024), https://www.herbertsmithfreehills.com/notes/tmt/2024-05/criminalising-deepfakes-the-uks-new-offences-following-the-online-safety-act.
170 *Criminalising Deepfakes – the UK's New Offences Following the Online Safety Act*, *supra* note 169.
171 *See id.*
172 *Id.*
173 *Id.*
174 Christy Cooney, *Creating Sexually Explicit Deepfakes to Become a Criminal Offence*, BBC (Apr. 16, 2024), https://www.bbc.com/news/uk-68823042.
175 *Criminalising Deepfakes – the UK's New Offences Following the Online Safety Act*, *supra* note 169.

The United Kingdom's approach to regulating artificial intelligence has been deemed neutral since the language used in the proposed legislation "does not refer to deepfakes but to the use of 'computer graphics or any other digital technology.'"[176] Further, instead of creating new laws, the United Kingdom's "approach has been to rely on existing legal frameworks to regulate [artificial intelligence], in efforts to avoid creating legislation which may become quickly outdated as [artificial intelligence] technologies advance."[177] Although there are strict laws protecting minors in the United Kingdom against the creation, distribution, and possession of deepfakes—with one perpetrator recently sentenced to eighteen years in prison[178]—this neutral approach taken by the country's legislators still leaves adult victims completely unprotected.

IV. SOLUTION

All across the globe, legislators are faced with two problems: (1) the rising amount of non-consensual sexually explicit deepfakes on the Internet and (2) how to regulate the spread of non-consensual porn generated by artificial intelligence. After analyzing the different approaches taken by several countries and the State of California, the best solution would be to create an independent, comprehensive, and new piece of legislation—not amending current legislation—to address the issue.

The legislation would include a prison term for those creating, distributing, and possessing non-consensual deepfakes of up to fifteen years if the victim is over eighteen years old and a prison term of up to twenty-five years if the victim is a minor. California bill AB-1831 should be incorporated into the legislation so that perpetrators can be prosecuted even if the material is not depicting a real child. Further, the legislation should impose five years of imprisonment for underage perpetrators if their conduct is willful.

In regard to civil liability, the legislation should include a section so that victims can seek redress of up to $300,000 plus punitive damages from their perpetrators and from any social media platform that played a part in facilitating the spread of deepfake material, as Telegram has done in South Korea. Additionally, the legislation should set regulations on social media platforms for them to implement better screening mechanisms to detect deepfakes, remove non-consensual sexually explicit deepfakes proactively—not after they receive a report from the victim—and report to authorities. Further, at least in the United States, Section 230 of the Communications Act should not be used as a defense to escape liability. Social media platforms that do not comply with the legislation should be subject to civil liability to the victims and be fined up to one million dollars.

---

[176] *Id.*

[177] *Id.*

[178] *See* Ewan Gawne, *Man Who Made 'Depraved' Child Images with AI Jailed*, BBC (Oct. 28, 2024), https://www.bbc.com/news/articles/cq6l241z5mjo.

All countries worldwide should adopt this type of legislation, independent of the legislation they already have in place, particularly so that offenders cannot escape justice if they are in a country with no statute on point. Victims of deepfakes have to live for the rest of their lives with the impacts of this new form of sexual abuse. All-encompassing and strict legislation is needed in order to address the issue properly.

V. CONCLUSION

Women and girls in every corner of the world are being victimized by the newest form of sexual abuse—deepfakes. Artificial intelligence is making it easy for perpetrators to sexually abuse women because now they do not even need a real nude photo to exploit and extort women and girls. Legislators across the world are grappling to pass legislation addressing the problem.

Currently, the most complete piece of legislation is in the State of California, with the only downfall being that it does not address punishment for perpetrators under the age of eighteen. The United States Congress is making good progress toward passing legislation, but there is still no law in place, and even then, they should attempt to pass one comprehensive piece of legislation addressing the issue, not several fragmented and scattered bills. On the other hand, the European Union takes a less proactive approach to combating deepfakes in its AI Act since it addresses the issue through disclosure requirements, and no law criminalizing non-consensual sexually explicit deepfakes has passed. In the case of South Korea, although they have laws in place criminalizing deepfakes, it is unlikely that they will bring perpetrators to justice due to the gender divide in the country. Further, the South Korean government does little to keep social media platforms accountable since it took no action against Telegram for failing to cooperate in 2020. Lastly, the United Kingdom's neutral approach toward artificial intelligence is also detrimental and leaves a significant gap between minor victims—who are protected—and adult victims—whose perpetrators currently can only receive a sentence of up to two years for sharing, not creating, deepfakes.

Non-consensual sexually explicit deepfakes are an epidemic. No current law or proposed legislation addresses the issue and its implications completely. Harsh prison sentences, high fines, civil recourse, and social media platform regulation and accountability must be in place to ensure that victims are adequately recompensed, perpetrators are punished, and social media platforms are held to higher transparency standards.