DEEP FAKES, DEEPER CONSEQUENCES: COMBATING AI CHILD PORNOGRAPHY BY MANDATING SEX OFFENDER REGISTRATION

Allison Mitton*

Abstract: Recent advancements in artificial intelligence and machine learning have led to deepfakes and AI-generated images being created and distributed at an unprecedented rate. While deepfakes are used for many purposes, the overwhelming majority are used to create non-consensual deepfake pornographic content depicting women and minors. This raises a critical issue: If deepfake pornography is so prevalent, how can the law effectively intervene to prevent more individuals from becoming victims? Shockingly, little to no effective federal legislation has been enacted to combat deepfake pornography—even when the images depict minors. I suggest that the most effective legislation would both (1) deter individuals from publishing deepfake pornography involving minors and (2) raise awareness of those who exploit others' images in violating ways. To accomplish this, I argue that the TAKE IT DOWN Act should be amended to include a provision requiring mandatory sex offender registration for those who publish deepfake pornography of minors. By incorporating this simple addition into a proposed federal law already poised for success, states can help prevent more people from becoming victims of deepfake pornography by publicly identifying individuals who may pose a threat.

Keywords: Deepfakes; Artificial Intelligence; Pornography

* J. Reuben Clark Law School, Brigham Young University, US.

Table of Contents

Introduction 113

I. Emergence of Deepfakes 114

A. Deepfakes and How They Work 114

B. The Dangers of Deepfakes 116

C. How Victims of Deepfake Pornography Are Affected 118

II. Current Remedies 119

A. Civil Remedies 119

1. Violation of Privacy Rights: False Light 120

2. Intentional Infliction of Emotional Distress 121

3. Defamation 121

4. Issues with Current Available Civil Remedies for Victims 123

B. Criminal Penalties 124

1. State Deepfake Pornography Laws 124

2. Legal Treatment of and Issues with Similar Crimes 125

III. Constitutional First Amendment Issues 127

A. Obscenity 127

B. Child Pornography 127

IV. Potential Solutions 128

A. Holding Tech Companies Liable 128

1. Social Media Restrictions 129

2. Amending Search Engine Algorithms 129

3. Section 230 Immunity 129

B. Proposed Federal Criminal Legislation 130

1. DEEP FAKES Accountability Act 131

2. TAKE IT DOWN Act 131

V. Amending the TAKE IT DOWN Act to Mandate Sex Offender Registration 133

A. Sex Offender Registries 133

B. Policy Considerations 135

Conclusion 136

INTRODUCTION

You are outraged. You just found out a classmate created a deepfake nude video of you and posted it online, where it's getting hundreds of views. You call the police, hoping for some help, but they tell you there is nothing they can do—to your horror, what happened to you is not considered a crime in the state you live in.

This nightmare scenario was a reality for Francesca Mani, a fourteen-year-old New Jersey high school student.[1] After being brought to her vice principal's office despite knowing she had done nothing wrong, she was told that she—and several other female peers—had been depicted in fake nude images created by male classmates, who then shared these images with many other students.[2]

Although, in theory, deepfake pornography could depict people of all genders, women are disproportionately victimized.[3] Many minors, including middle and high school-aged girls, have been put on display in forged pornography created by predators or even their own peers.[4]

Because of recent advancements in artificial intelligence (AI) and machine learning, more deepfake pornography is being made now than ever.[5] According to experts, "[t]here are 550% more deepfake videos online in 2023 than in 2019," with a 464% increase in deepfake pornography between 2022 and 2023 alone.[6]

Although the problem of deepfake pornography has become so rampant, little to no effective legislation has been passed to help resolve the issue.[7] Shockingly, less

---

[1] Jessica Le Masurier, '*A Global Problem': US Teen Fights Deepfake Porn Targeting Schoolgirls*, FRANCE 24 (Apr. 18, 2024, 1:31 PM), https://www.france24.com/en/tv-shows/focus/20240418-a-global-problem-us-teen-fights-deepfake-porn-targeting-schoolgirls.

[2] *Id.*

[3] 99% of deepfake pornography depicts women. *See, e.g., 2023 State of Deepfakes*, SECURITY HERO, https://www.securityhero.io/state-of-deepfakes/#:~:text=Between%202022%20%26%202023%2C%20the%20amount,year%20was%20a%20startling%20464%25 (last visited Oct. 12, 2024); Arwa Mahdawi, *Nonconsensual Deepfake Porn is an Emergency that Is Ruining Lives*, THE GUARDIAN (Apr. 1, 2023, 9:00 AM), https://www.theguardian.com/commentisfree/2023/apr/01/ai-deepfake-porn-fake-images.

[4] *See generally* Kat Tenbarge, *Beverly Hills Middle School Expels 5 Students After Deepfake Nude Photos Incident*, NBC NEWS (Mar. 8, 2024, 11:55 AM), https://www.nbcnews.com/tech/tech-news/beverly-hills-school-expels-students-deepfake-nude-photos-rcna142480 (explaining that five eighth grade boys were expelled from a school in Beverly Hills, California, after creating and sharing deepfake pornographic images of sixteen of their female classmates); 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 (stating that "[m]ost suspected perpetrators [of creating deepfake pornography] in South Korea are teenage boys . . . [who] target female friends, relatives and acquaintances—also mostly minors—as a prank, out of curiosity or misogyny.").

[5] *See, e.g.,* Stu Sjouwerman, *Exponential Deepfake Porn is Out of Control and a Huge Security Risk*, KNOWBE4 (Oct. 16, 2024), https://blog.knowbe4.com/exponential-deepfake-porn-is-out-of-control-and-a-huge-security-risk; *2023 State of Deepfakes*, *supra* note 3.

[6] *2023 State of Deepfakes*, *supra* note 3.

[7] *See, e.g.,* Le Masurier, *supra* note 1; Andrew R. Chow, *Francesca Mani: Anti-Deepfake Activist*, TIME (Sept. 5, 2024, 7:17 AM), https://time.com/7012803/francesca-mani; Michelle M. Graham, *Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat*, THOMSON REUTERS (June 26, 2024), https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation; *contra Most States Have Enacted Sexual Deepfake Laws*, MULTISTATE AI (June 28, 2024),

than half of states have passed legislation restricting "the distribution of nonconsensual sexual deepfakes,"[8] and, as of this writing, no federal legislation has been passed to regulate deepfake pornography yet—even when it depicts minors.[9]

This Note argues that the current available remedies for victims of deepfake pornography pose challenges due to their heavy reliance on civil law and the inconsistency of state criminal laws, so it is imperative for states to help prevent more people from becoming victims by publicly identifying individuals who may pose a threat through sex offender registries. To do so, a provision should be added to the proposed TAKE IT DOWN Act to mandate sex offender registration for those who publish deepfake pornography featuring minors.

Part I gives a brief background on the emergence of deepfakes and how they operate. Part II will discuss the current available civil and criminal remedies for victims of deepfake pornography. Part III describes constitutional First Amendment issues which pose an obstacle to passing legislation. Part IV describes solutions others have offered, including holding tech companies liable and federal proposed legislation. Finally, Part V argues that the TAKE IT DOWN Act should be amended to include mandatory sex offender registration for those who publish deepfake pornography featuring minors and outlines a simple approach for its implementation.

I. EMERGENCE OF DEEPFAKES

A. Deepfakes and How They Work

Deepfakes are forged videos or images "created via deep learning,[10] a form of artificial intelligence, where a person's likeness, including their face and voice, can be realistically swapped with someone else's."[11] The term "deepfake" was first coined in 2017, when a person under the username "deepfakes" started posting deepfake celebrity pornography on Reddit.[12] The term itself is a portmanteau of the words "deep" (to signal that it was created through deep-learning AI technology) and "fake" (to signal that the content was created using AI).[13]

---

https://www.multistate.ai/updates/vol-32 (stating that most states have passed enacted laws; however, these solutions are ineffective).

[8] *Most States Have Enacted Sexual Deepfake Laws*, *supra* note 7. *See also* Graham, *supra* note 7, *Can State Laws Actually Stop Political Deepfakes?*, MULTISTATE AI (Apr. 15, 2024), https://www.multistate.ai/updates/vol-22; *Dozens of AI Laws Go Into Effect*, MULTISTATE AI (July 12, 2024), https://www.multistate.ai/updates/vol-33.

[9] Graham, *supra* note 7.

[10] For more information on deep learning generally, see *What is Deep Learning?*, AMAZON WEB SERVICES, https://aws.amazon.com/what-is/deep-learning (last visited Oct. 16, 2024) ("Deep learning is a method in artificial intelligence (AI) that teaches computers to process data in a way that is inspired by the human brain. Deep learning models can recognize complex patterns in pictures, text, sounds, and other data to produce accurate insights and predictions.").

[11] *Deepfake Technology*, ORG. FOR SOC. MEDIA SAFETY, https://www.socialmediasafety.org/advocacy/deepfake-technology (last visited Oct. 5, 2024).

[12] *See, e.g., id.*; Laura Payne, *Deepfake*, BRITTANICA (Oct. 1, 2024), https://www.britannica.com/technology/deepfake; Meredith Somers, *Deepfakes, Explained*, MIT MGMT. SLOAN SCH. (July 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

[13] Payne, *supra* note 12.

The typical process of creating a deepfake face-swapping video is done in several steps.[14] First, "thousands[15] of face shots of the two people [must be] run through an AI algorithm called an encoder. The encoder finds and learns similarities between the two faces, and reduces them to their shared common features, compressing the images in the process."[16] This process essentially creates a "lower dimensional representation" of each face, which at this point, "might not look like . . . face[s] at all."[17] Next, each image passes through a second algorithm called a decoder.[18] Normally during this step, each decoder reconstructs the original image it was given, making the images look more like real faces again.[19] Face swapping, on the other hand, takes place when the encoded images are fed into the opposite decoder (i.e., when "a compressed image of person A's face is fed into the decoder trained on person B . . . [so that] the face of person B [is reconstructed] with the expressions and orientation of [person] A").[20] The result is a forged but realistic-looking face.

Face-swapping is not the only way false images can be made, though—generative AI also enables users to create images with only a single photo or even from scratch.[21] By using the same AI systems as face-swapping programs, people can "animate one or several photos of people by first training an AI system on a dataset of videos including many celebrities, so it could learn about key points on the face."[22]

Even without a reference image, people can use generative AI to make new images.[23] To create images from scratch, "machine learning model[s] scan[] millions of images across the internet along with the text associated with them."[24] The algorithms are able to "spot trends in the images and text and eventually guess which

---

[14] *See* Ian Sample, *What Are Deepfakes – And How Can You Spot Them?*, THE GUARDIAN (Mar. 3, 2023), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them. The author explains that deepfakes can also be created through generative adversarial networks, or GANs. The author describes: "A G[AN] pits two artificial intelligence algorithms against each other. The first algorithm, known as the generator, is fed random noise and turns it into an image. This synthetic image is then added to a stream of real images—of celebrities, say—that are fed into the second algorithm, known as the discriminator." Although the images will not look like real faces at first, repeating the process eventually results in extremely realistic faces.

[15] In the past, thousands of images used to be required to create a deepfake, but now not as many are required. *See* Stuart A. Thompson, *Making Deepfakes Gets Cheaper and Easier Thanks to A.I.*, N.Y. TIMES (Mar. 12, 2023), https://www.nytimes.com/2023/03/12/technology/deepfakes-cheapfakes-videos-ai.html.

[16] Sample, *supra* note 14.

[17] Alan Zucconi, *Understanding the Technology Behind DeepFakes*, ALAN ZUCCONI (Mar. 14, 2018), https://www.alanzucconi.com/2018/03/14/understanding-the-technology-behind-deepfakes.

[18] *See, e.g.,* Sample, *supra* note 14; Zucconi, *supra* note 17.

[19] *Id.*

[20] Sample, *supra* note 14.

[21] *See, e.g.,* Sarah Morrison, *How Unbelievably Realistic Fake Images Could Take Over the Internet*, VOX (Mar. 30, 2023, 4:30 AM), https://www.vox.com/technology/2023/3/30/23662292/ai-image-dalle-openai-midjourney-pope-jacket; Rachel Metz, *Researchers Can Now Use AI and Make Fake Videos of Anyone*, CNN: BUSINESS (May 24, 2019, 7:40 PM), https://www.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html.

[22] Metz, *supra* note 21.

[23] *See Free Online Image Generator*, CANVA, https://www.canva.com/ai-image-generator (last visited Nov. 5, 2024).

[24] *Id.*

image and text fit together."[25] After the model learns what a prompt's given image should look like, it can generate a new image.[26]

Because images created using generative AI are so similar to forged images created by face-swapping, and because legislation tends to refer to deepfakes and AI-generated images interchangeably,[27] this Note refers to both types of images as deepfakes.

B. The Dangers of Deepfakes

Although deepfakes can be used for fun,[28] they can—and often are—used for much more nefarious purposes.[29] They are frequently used in scamming schemes (through replicating a person's voice or image to convince those they know or work with to transfer money)[30] or to otherwise distribute misinformation, especially

---

[25] *Id.*
[26] *Id.*
[27] *See* TAKE IT DOWN Act, S. 4569, 188th Congress (2024).
[28] *See generally* Rob Cover, *Celebrity Deepfakes Are All Over TikTok. Here's Why They're Becoming Common – And How You Can Spot Them*, THE CONVERSATION (July 18, 2022, 4:05 PM), https://theconversation.com/celebrity-deepfakes-are-all-over-tiktok-heres-why-theyre-becoming-common-and-how-you-can-spot-them-187079 (stating that deepfakes have been used in "silly videos featuring actors such as Robert Pattinson[,] . . . Keanu Reeves[, and Tom Cruise]"); Simon Ellery, *Fake Photos of Pope Francis in a Puffer Jacket Go Viral, Highlighting the Power and Peril of AI*, CBS NEWS (Mar. 28, 2023, 11:39 AM), https://www.cbsnews.com/news/pope-francis-puffer-jacket-fake-photos-deepfake-power-peril-of-ai (noting a deepfake image of Pope Francis wearing "a stylish white puffer jacket and silver bejewelled crucifix" that went viral on social media).
[29] *See generally* Sophie Compton & Reuben Hamlyn, *Opinion: The Rise of Deepfake Pornography Is Devastating for Women*, CNN (Oct. 29, 2023, 12:07 PM), https://www.cnn.com/2023/10/29/opinions/deepfake-pornography-thriving-business-compton-hamlyn/index.html (explaining that the majority of deepfake videos are pornographic); Kat Tenbarge, *Found Through Google, Bought With Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 9:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 (same); Stuart A. Thompson, *How 'Deepfake Elon Musk' Became the Internet's Biggest Scammer*, N.Y. Times (Aug. 14, 2024), https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html (explaining how a deepfake video of Elon Musk was used in a scam); Dylan Butts, *Deepfake Scams Have Robbed Companies of Millions. Experts Warn It Could Get Worse*, CNBC (May 27, 2024, 10:20 PM), https://www.cnbc.com/2024/05/28/deepfake-scams-have-looted-millions-experts-warn-it-could-get-worse.html (stating that "deepfake scans ha[ve] looted millions of dollars from companies worldwide"); Alexei Alexis, *Deepfake Scams Escalate, Hitting 53% of Businesses*, CFO DIVE (Sept. 3, 2024), https://www.cfodive.com/news/deepfake-scams-escalate-hitting-53-percent-of-businesses/725836 (explaining that most businesses have been targets of deepfake scams); Heather Chen & Kathleen Magramo, *Finance Worker Pays Out $25 Million After Call with Deepfake 'Chief Financial Officer'*, CNN: WORLD (Feb. 4, 2024, 2:31 AM), https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html (describing how a realistic deepfake led an employee to pay millions to a scammer).
[30] *See generally* Butts, *supra* note 28 (mentioning that "the chief executive officer of a British energy provider reportedly transferred £220,000 ($238,000) to a scammer who had digitally mimicked the head of his parent company and asked for a wire to a supposed supplier on a phone call"); Thompson, *supra* note 28 (explaining that Elon Musk "was featured in nearly a quarter of all deepfake scams since late [2023]"); Chen & Magramo, *supra* note 28 (describing an incident where "[a] finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call"). *See also* Alexis, *supra* note 28 (explaining that 53% of U.S. and U.K. businesses "have been targets of a financial scam powered by 'deepfake' technology, with 43% falling victim to such attacks").

politically.[31] But the overwhelming majority of deepfakes are used to create pornographic videos—according to a company that monitors AI-developed content, a whopping "96% of deepfakes are sexually explicit and feature women who didn't consent to the videos."[32]

Deepfakes are especially dangerous because the videos can "cost as little as $10 to create" and can be made "in less than [ten] minutes."[33] Less realistic deepfake videos can even be created "for free in less than [thirty] seconds."[34] A quick Google search for deepfake video creation apps returns several popular options, with only some prohibiting users from creating pornographic images of others. People seeking to create deepfake pornography who feel it may be too risky to use these websites or apps on their own may also turn to more experienced deepfake creators advertising their services on platforms like Discord,[35] Reddit,[36] and Telegram[37] to create the videos for them.

---

[31] *See generally* Em Steck & Andrew Kaczynski, *Fake Joe Biden Robocall Urges New Hampshire Voters Not to Vote in Tuesday's Democratic Primary*, CNN: POLITICS (Jan. 22, 2024, 5:44 PM), https://www.cnn.com/2024/01/22/politics/fake-joe-biden-robocall/index.html (detailing an incident of a fake robocall using Joe Biden's voice to tell voters not to vote in a Democratic primary); Matt Brown & David Klepper, *Fake Images Made to Show Trump With Black Supporters Highlight Concerns Around AI and Elections*, AP NEWS (Mar. 7, 2024, 10:09 PM), https://apnews.com/article/deepfake-trump-ai-biden-tiktok-72194f59823037391b3888a1720ba7c2 (explaining how fabricated images of "Donald Trump surrounded by groups of Black people smiling and laughing" sought to influence the voting behaviors of Black voters). In fact, so many deepfakes have been used to distribute political misinformation that scholars at Purdue University have created a database, called the Political Deepfakes Incidents Database (PDID), to track them. Andrea Azzo, *Tracking Political Deepfakes: New Database Aims to Inform, Inspire Policy Solutions*, NW.: CTR. FOR ADVANCING SAFETY OF MACH. INTEL. (Jan. 26, 2024), https://casmi.northwestern.edu/news/articles/2024/tracking-political-deepfakes-new-database-aims-to-inform-inspire-policy-solutions.html.

[32] Sophie Compton & Reuben Hamlyn, *Opinion: The Rise of Deepfake Pornography Is Devastating for Women*, CNN (Oct. 29, 2023, 12:07 PM), https://www.cnn.com/2023/10/29/opinions/deepfake-pornography-thriving-business-compton-hamlyn/index.html; Kat Tenbarge, *Found Through Google, Bought With Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 9:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071.

[33] Thompson, *supra* note 28.

[34] Lutz Finger, *Overview of How to Create Deepfakes – It's Scarily Simple*, FORBES (Sept. 8, 2022, 10:09 AM), https://www.forbes.com/sites/lutzfinger/2022/09/08/overview-of-how-to-create-deepfakesits-scarily-simple.

[35] *See generally* Kat Tenbarge, *Found Through Google, Bought With Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, 9:56 AM), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 (explaining that one Discord user advertised that he could create a five-minute long "deepfake of a 'personal girl,' meaning anyone with fewer than [two] million Instagram followers, for $65.").

[36] Deepfakes themselves originated from a Reddit community, as discussed in Part I(A). *See, e.g., Deepfake Technology, Org. for Soc. Media Safety, https://www.socialmediasafety.org/advocacy/deepfake-technology (last visited Oct. 5, 2024); Laura Payne, Deepfake, Brittanica (Oct. 1, 2024), https://www.britannica.com/technology/deepfake;* Meredith Somers, *Deepfakes, Explained*, MIT MGMT. SLOAN SCH. (July 21, 2020), https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.

[37] *See generally* Bill Goodwin, *Deep Fake AI Services on Telegram Pose Risk for Elections*, COMPUTERWEEKLY.COM (Mar. 18, 2024, 12:00 PM), https://www.computerweekly.com/news/366574113/Deep-fake-AI-services-on-Telegram-pose-risk-for-elections (explaining that "[s]ecurity analysts have identified more than 400 channels promoting

Many deepfake videos feature celebrities, because they are well-known and because there are hundreds—if not, thousands—of readily available photos that can be used to generate the deepfake video.[38] However, because deepfake technology has become more advanced over the years and no longer requires such large datasets,[39] deepfake pornography also now commonly features non-celebrities.[40]

In fact, "[w]ith just a single good image of a person's face, it is now possible . . . to make a 60-second [pornographic] video of that person."[41] Unsurprisingly, because most people have social media accounts with plenty of high-quality images of themselves publicly available, many deepfake creators get the images they use from their victims' social media profiles or the social media profiles of others[42]—yet many people are likely unaware of the potential dangers associated with sharing their images (or images of their children) publicly online.[43]

C. How Victims of Deepfake Pornography Are Affected

Deepfake pornography creators are hard to pin down because most of the time, the images and videos are uploaded by anonymous users.[44] As a result, victims can "feel isolated, disconnected, and mistrustful of many people around them [and] are likely to experience poor mental health symptoms like depression and anxiety."[45] In any case, including when the victim knows who created the deepfake,[46] victims

---

deep fake services on the Telegram Messenger app, ranging from automated bots that help users create deep fake videos to individuals offering to create bespoke fake videos.").

[38] See Ben Dickson, *What Are Deepfakes?*, TECHTALKS (Sept. 4, 2020), https://bdtechtalks.com/2020/09/04/what-is-deepfake, explaining that "[t]he need for large datasets is why most deepfake videos you see target celebrities. You can't create a deepfake of your neighbor unless you have hours of videos of them in different settings."

[39] *See generally* Stuart A. Thompson, *Making Deepfakes Gets Cheaper and Easier Thanks to A.I.*, N.Y. TIMES (Mar. 12, 2023), https://www.nytimes.com/2023/03/12/technology/deepfakes-cheapfakes-videos-ai.html (explaining that the creation of deepfakes "once required elaborate software to put one person's face onto another's[, b]ut now, many of the tools to create them are available to everyday consumers—even on smartphone apps, and often for little to no money."); Andrea Hauser, *Deepfakes Analysis: Amount of Images, Lighting, and Angles*, SCIP, https://www.scip.ch/en/?labs.20181122 (last visited Oct. 6, 2024) (noting that "[the amount of faces plays less of a role than [she] expected. Much more important is the similarity of the [images] in terms of illumination and angles of the faces.").

[40] *See, e.g.,* Vittoria Elliott, *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.

[41] Nicholas Kristof, *The Online Degradation of Women and Girls That We Meet With a Shrug*, N.Y. TIMES (Mar. 23, 2024), https://www.nytimes.com/2024/03/23/opinion/deepfake-sex-videos.html.

[42] *See, e.g.,* Gina Silva, *Stolen Instagram Pics Used in Deepfake AI Porn: What to Know*, FOX 11 L.A. (Jan. 31, 2024, 8:38 AM), https://www.foxla.com/news/la-women-victims-of-deepfake-ai-porn; Jillian Krasusky, *Someone Might Be Using Your Instagram Stories to Make Deepfake Porn*, MEDIUM (Apr. 13, 2022), https://medium.com/art-of-the-argument/someone-might-be-using-your-instagram-stories-to-make-deepfake-porn-310ff06b6481.

[43] *See generally* Jim Axelrod, Teen victim of AI-generated "deepfake pornography" urges Congress to pass "Take It Down Act", CBS NEWS (Dec. 18, 2024, 7:47 PM), *https://www.cbsnews.com/news/deepfake-pornography-victim-congress* (describing a story of a teen who was shocked when a classmate used an image from her Instagram account to create a forged naked photo of her).

[44] *See* Krasusky, *supra* note 41.

[45] Halle Nelson, *Taylor Swift and the Dangers of Deepfake Pornography*, NAT. SEXUAL VIOLENCE RES. CTR. (Feb. 7, 2024), https://www.nsvrc.org/blogs/feminism/taylor-swift-and-dangers-deepfake-pornography.

[46] Many teenagers who create deepfake pornography do so as a "prank" toward their female friends, acquaintances, or classmates. In these scenarios, the victims usually know who created the deepfake,

experience extreme distress and humiliation.[47] Victims also are likely to experience reputational damage, with some even losing their jobs or missing out on future employment prospects because of the online permanency of the images.[48] Some victims are so humiliated that they attempt suicide or take their own lives because they no longer want to suffer from the horrible and unjust consequences they face.[49]

Because victims of deepfake pornography face such serious and horrific consequences, lawmakers and society at large must address this issue and, where possible, notify potential victims about individuals in their communities who previously created or possessed deepfake pornography.

II. CURRENT REMEDIES

While holding the tech companies liable who permit this content to be spread may seem like an obvious solution, they are currently protected from liability for third-party content posted to their sites under Section 230 of the Communications Decency Act, as discussed below in Part IV(A)(3). As a result, adult victims of deepfake pornography are currently only able to rely on general civil law.[50]

Lawsuit claims could be "filed for defamation, invasion of privacy, [or intentional infliction of] emotional distress."[51] For such a lawsuit to succeed, "victims must prove that the deepfake was false, was made with reckless disregard for the truth, and caused harm to their reputation or finances."[52] If they do so, victims can receive monetary damages or injunctions—ideally, the creator would take the deepfake images off the internet to prevent further harm from occurring.[53]

Beyond civil remedies, creators of deepfake pornography may also face criminal penalties. Victims, however, have no control over prosecution of these crimes, as this responsibility is one that lies with the government.[54]

A. Civil Remedies

---

since the creator does not try to hide it. *See* Jessica Le Masurier, *'A Global Problem': US Teen Fights Deepfake Porn Targeting Schoolgirls*, FRANCE 24 (Apr. 18, 2024, 1:31 PM), https://www.france24.com/en/tv-shows/focus/20240418-a-global-problem-us-teen-fights-deepfake-porn-targeting-schoolgirls; 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.

[47] *See* Nelson, *supra* note 45.

[48] Nelson, *supra* note 45. *See, e.g.,* Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do*, N.Y. TIMES (July 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html (describing how "a rising star in local politics" feared her career would be over if she lost "the respect of her older colleagues").

[49] Kim, *supra* note 43.

[50] As discussed below in Part II(B)(1), possessing deepfake child pornography can be prosecuted under criminal law in some states.

[51] *Legal Remedies for Deepfake Victims: Guide*, SCOREDETECT: BLOG (June 29, 2024), https://www.scoredetect.com/blog/posts/legal-remedies-for-deepfake-victims-guide.

[52] *Id.*

[53] *See* Danielle Keats Citron, *Privacy Injunctions*, 71 EMORY L.J. 955, 970–72 (2022).

[54] *Criminal Cases*, U.S. COURTS, https://www.uscourts.gov/about-federal-courts/types-cases/criminal-cases (last visited Nov. 12, 2024).

Civil remedies may include claims for violation of privacy rights, intentional infliction of emotional distress, and defamation. However, as discussed below, none of these options offers an ideal solution, as their requirements are typically difficult to satisfy.[55]

1. Violation of Privacy Rights: False Light

First, victims may sue under violation of privacy rights, which are generally understood as "the right to be let alone."[56] Though most people consider deepfake pornography to be a violation of privacy[57] because it "annihilates victims' sexual privacy and inherently strips [victims] of their humanity,"[58] privacy-based torts may not offer the best solution for victims. Privacy can be invaded in several ways, including "intrusion on seclusion, wrongful appropriation, false light, and public disclosure of private fact."[59] However, given the elements for each, only false light is likely to meet the requirements.

False light torts aim to hold accountable those who portray others in a misleading way.[60] Under this approach, individuals are considered liable for invasion of privacy if (1) "the false light in which the other was placed would be highly offensive to a reasonable person," and (2) "the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[61]

With deepfake pornography, the first element is likely satisfied, as most would consider such videos to be highly offensive.[62] The second element, however, is much more challenging to meet.[63] Many deepfake videos are low-quality and easily recognized as fake by viewers,[64] which would not place the victim in a false light. However, a creator of high-quality deepfake videos could attempt to avoid liability by simply labeling the video as fake, because with such a disclaimer, "the portrayal cannot be taken seriously as an accurate depiction."[65]

---

[55] Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 Vand. L. Rev. 1479 (2020).

[56] Restatement 2d of Torts, § 652A, comment a.

[57] A study indicates that 68% of individuals "would feel shocked and outraged by the violation of someone's privacy and consent in the creation of deepfake pornographic content." *2023 State of Deepfakes*, SECURITY HERO, https://www.securityhero.io/state-of-deepfakes/#:~:text=Between%202022%20%26%202023%2C%20the%20amount,year%20was%20a%20startling%20464%25 (last visited Nov. 9, 2024).

[58] Gieseke, *supra* note 54, at 1483.

[59] *Id.* at 1496; Restatement 2d of Torts, § 652A.

[60] *See* Restatement 2d of Torts, § 652E.

[61] Restatement 2d of Torts, § 652E.

[62] *See, e.g.,* Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do*, N.Y. TIMES (July 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html; Halle Nelson, *Taylor Swift and the Dangers of Deepfake Pornography*, NAT. SEXUAL VIOLENCE RES. CTR. (Feb. 7, 2024), https://www.nsvrc.org/blogs/feminism/taylor-swift-and-dangers-deepfake-pornography.

[63] See Gieseke, *supra* note 54, at 1498.

[64] *See, e.g.,* Gieseke, *supra* note 54, at 1498; Ian Sample, *What Are Deepfakes – And How Can You Spot Them?*, THE GUARDIAN (Mar. 3, 2023), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

[65] Gieseke, *supra* note 54, at 1498.

2. Intentional Infliction of Emotional Distress

Victims may also sue under the tort claim of intentional infliction of emotional distress (IIED). An action for IIED can be brought when (1) "[t]he defendant intended to inflict emotional distress or . . . knew or should have known that emotional distress was likely to result from [their] conduct;" (2) "[t]he defendant's conduct was extreme and outrageous;" (3) "[t]he defendant's conduct was the cause of the plaintiff's emotional distress;" and (4) "[t]he emotional distress sustained by the plaintiff was severe."[66]

Although this may seem like a viable option, it is difficult to meet most of these requirements. First, it can be difficult to prove that the creator intended, knew, or should have known that emotional distress was likely to result from their conduct, as many deepfakes are created for private use[67] or are created to merely "prank" the victim.[68]

Next, the conduct must be extreme and outrageous. Conduct meets this requirement when it is "so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community."[69] This element is likely met because a reasonable person would consider deepfake pornography to go beyond the bounds of decency.[70]

However, it may be difficult to prove the final element: that the emotional distress the victim experiences is severe. The definition of severe depends on the jurisdiction, but many consider emotional distress to be severe when "the distress inflicted is so extreme that no reasonable [person] could be expected to endure it without undergoing unreasonable suffering."[71] Certainly many victims of deepfake pornography experience this unreasonable level of suffering,[72] but for victims who are merely embarrassed and want the deepfake taken down, this element would not be met.

3. Defamation

Defamation may be the most effective option for victims of deepfake pornography, but it still presents a challenging standard to meet.[73] For a victim to sue for defamation, they must prove that (1) "[t]he defendant made a false and defamatory statement concerning the plaintiff;" (2) "[t]he statement was published to a third party;"

---

[66] 1 Jury Instructions on Damages in Tort Actions § 7.09.
[67] The Yatterbog, *Deepfakes: Public vs Personal Use*, MEDIUM (Dec. 1, 2023), https://medium.com/@yatterbog/deepfakes-public-vs-personal-use-b48e55bff745.
[68] *See generally* 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 (stating that "[m]ost suspected perpetrators [of creating deepfake pornography] in South Korea are teenage boys . . . [who] target female friends, relatives and acquaintances—also mostly minors—as a prank, out of curiosity or misogyny.").
[69] Restatement 2d of Torts, § 46, comment d.
[70] *See* Gieseke, *supra* note 54 at 1499.
[71] Tidelands Auto. Club v. Walters, 699 S.W.2d 939, 941 (Tex. App. 1985).
[72] *See* Halle Nelson, *Taylor Swift and the Dangers of Deepfake Pornography*, NAT. SEXUAL VIOLENCE RES. CTR. (Feb. 7, 2024), https://www.nsvrc.org/blogs/feminism/taylor-swift-and-dangers-deepfake-pornography.
[73] Emma Grey Ellis, *People Can Put Your Face on Porn—and the Law Can't Help You*, WIRED (Jan. 26, 2018, 7:00 AM), https://www.wired.com/story/face-swap-porn-legal-limbo.

(3) [t]here was . . . negligence, intent, or actual malice on the part of the defendant;" and (4) "[t]he plaintiff suffered harm to [their] reputation."[74]

For a statement to be considered defamatory, the statement must "harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[75] Embarrassing or frustrating the plaintiff is not enough—the statement "must provoke the kind of harm which has grievously fractured [one's] standing in the community of respectable society."[76]

When deepfake pornography is shared with others, the first two requirements are typically met: the content of the video is considered a false statement, and posting or otherwise sharing it fulfills the publication requirement.[77] Not every jurisdiction treats the publication requirement the same, but most require the statement to be seen or heard by a third party. For example, New Mexico considers publication to be "an intentional or negligent communication to one other than the person defamed,"[78] meaning that even if the content is not posted publicly but rather shared privately to someone else, it could still meet the publication requirement. Because deepfake pornography can be distributed via text messages or social media chat services like Snapchat and can easily be displayed to others in person,[79] the publication requirement would likely be met.

However, requiring the producer to have negligence, intent, or actual malice demonstrates a limitation of this approach. No uniform standard for each of these terms exists, and definitions may differ from one jurisdiction to another.[80] Generally, negligence is defined as "the failure to do what a reasonable and prudent person would ordinarily have done under the circumstances of the situation."[81] Intent refers to "the purpose formed in [one's] mind,"[82] while some jurisdictions define actual malice as acting with "spite and ill will . . . with a design willfully or wantonly to injure another."[83] While the standard for negligence may be achievable, proving intent or actual malice would be challenging to prove, because as one scholar notes, "many producers have no idea the victim will ever discover the video [and] neither intend emotional distress nor reasonably know that their deepfake winds up in the victim's hands."[84]

---

[74] 1 Jury Instructions on Damages in Tort Actions § 12.03A.
[75] Graboff v. Colleran Firm, 744 F.3d 128, 136 (2014) (quoting Tucker v. Fishchbein, 237 F.3d 275, 282 (2001)).
[76] *Id.* (quoting Tucker v. Phila. Daily News, 577 Pa. 598, 615 (2004)).
[77] Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 Vand. L. Rev. 1479, 1500 (2020).
[78] 13-1003 NMRA.
[79] Jessica Le Masurier, *'A Global Problem': US Teen Fights Deepfake Porn Targeting Schoolgirls*, FRANCE 24 (Apr. 18, 2024, 1:31 PM), https://www.france24.com/en/tv-shows/focus/20240418-a-global-problem-us-teen-fights-deepfake-porn-targeting-schoolgirls.
[80] 1 Jury Instructions on Damages in Tort Actions § 12.03A, comment 3.
[81] 13B M.J. Negligence § 2 (2024).
[82] 9B M.J. Homicide § 34 (2024).
[83] Heuer v. John R. Thompson Co., 251 S.W.2d 980, 986 (Mo. Ct. App. 1952).
[84] Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 Vand. L. Rev. 1479, 1500 (2020).

Last, plaintiffs must suffer harm to their reputation.[85] While many victims face reputational harm—such as when deepfake pornography appears in internet searches associated with their name—some victims might not.[86] For example, minors who are sexually promiscuous or who have taken consensual nude photographs of themselves may be denied relief because similar images of them already exist, perhaps leading to the perception that their reputation has not been harmed.[87]

4. Issues with Current Available Civil Remedies for Victims

Overall, litigation is an unfair solution for victims of deepfake pornography. Although there are countless victims of deepfake pornography, only two civil lawsuits have been filed to date over deepfake pornography as of this writing—and one was brought by San Francisco's City Attorney, not by a victim directly.[88] Part of this disparity can be attributed to the likelihood that many potential cases are filtered out for the reasons mentioned above. However, even when all elements of a given civil remedy can be established, civil lawsuits likely remain rare due to the many barriers to litigation.

One barrier is that litigation is notoriously time-consuming and expensive.[89] When online content is the subject of a legal dispute, attorneys or digital forensics experts must be consulted,[90] which only increases these costs. Many people, including minors who rely on their parents, have neither the resources nor the time to pursue litigation. Moreover, civil litigation typically compensates victims monetarily, as injunctions are rarely granted—but most victims just want the deepfake content removed from the internet and deleted permanently.

Apart from these issues, civil litigation does not provide the penalties criminal law does. Litigation is time-consuming and costly for defendants, too, but that alone does little to deter perpetrators from publishing deepfake pornography of others in the future, given how infrequently victims pursue litigation. Although involvement in civil lawsuits must be disclosed in situations like background checks and certain insurance or credit applications, this level of disclosure does not carry the same public awareness as a criminal charge.

---

[85] 1 Jury Instructions on Damages in Tort Actions § 12.03A.

[86] *See* Sophie Compton & Reuben Hamlyn, *Opinion: The Rise of Deepfake Pornography is Devastating for Women*, CNN (Oct. 29, 2023, 12:07 PM), https://www.cnn.com/2023/10/29/opinions/deepfake-pornography-thriving-business-compton-hamlyn/index.html.

[87] *See* Camille Sojit Pejcha, *Deepfake Porn Isn't Just a Consent Issue, It's a Labor Issue*, DOCUMENT (Feb. 2, 2023), https://www.documentjournal.com/2023/02/twitch-streamer-deepfake-controversy-ai-porn-sex-work-labor-technology (explaining that some may think "sex worker[s] [are] essentially considered to be 'asking for it' by participating in sex work").

[88] This lawsuit seeks to permanently shut down sixteen popular websites that create AI pornography of women. Isaiah Poritz, *San Francisco Files Nation's First Suit Over AI Pornography*, BLOOMBERG LAW (Aug. 15, 2024, 11:50 AM), https://news.bloomberglaw.com/litigation/san-francisco-files-nations-first-suit-over-ai-generated-porn. The only other lawsuit that has been filed is Francesca Mani's case mentioned in Part I.

[89] Sam Bock, *4 Barriers Blocking Access to Justice (and How to Help Break Them)*, RELATIVITY: BLOG (Mar. 25, 2021), https://www.relativity.com/blog/4-barriers-blocking-access-to-justice-and-how-to-break-them.

[90] *Legal Remedies for Deepfake Victims: Guide*, SCOREDETECT: BLOG (June 29, 2024), https://www.scoredetect.com/blog/posts/legal-remedies-for-deepfake-victims-guide.

While civil litigation can be a viable option for victims who manage to overcome these barriers, it is evident that the existing civil remedies available to victims do not fully address the problem.

B. Criminal Penalties

In addition to civil laws, criminal laws may penalize those who create or distribute deepfake pornography under certain circumstances. While there are no federal criminal laws specifically prohibiting deepfake pornography,[91] certain states have created their own laws—typically modeled after their legal treatment of similar crimes—or have "expanded existing crimes to cover these acts."[92]

1. State Deepfake Pornography Laws

Many states have recognized the dangers of deepfakes and have either initiated or enacted laws to address the problem, while others have attempted to enact legislation but have not succeeded.[93] These state laws differ widely in their definitions of key terms, overall regulations, and associated penalties.

First, key terms are defined differently. To illustrate, Mississippi defines "intimate part" as "the naked genitals, pubic area, anus[,] or female nipple of the person,"[94] while Illinois expands this definition to include parts that are "fully unclothed, partially unclothed, or transparently clothed" and "partially or fully exposed."[95] Illinois includes the same intimate parts as Mississippi, but it limits female nipples to only include "post-pubescent nipple[s]," which poses an issue for images depicting minors.[96]

Overall regulations also vary widely. For example, Alabama criminalizes creating an AI image if the person "knowingly creates, records, or alters a private image when the depicted individual has not consented to the creation, recording, or alteration and the depicted individual had a reasonable expectation of privacy."[97] New York similarly criminalizes "dissemination or publication of an intimate image," but adds more requirements—the perpetrator must "inten[d] to cause harm to the emotional, financial or physical welfare of another" and the image must depict "one or more intimate parts" of a person or someone "engaging in sexual conduct with another."[98]

Some states have also enacted laws specifically criminalizing deepfake child pornography. For instance, South Dakota recently enacted a law providing that "a person is guilty of possessing child pornography if the person knowingly possesses any

---

[91] Rebecca Pirius, *Is Deepfake Pornography Illegal?*, CRIM. DEF. LAW. (Sept. 26, 2024), https://www.criminaldefenselawyer.com/resources/is-deepfake-pornography-illegal.html.
[92] *Id.*
[93] *Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation*, NCSL (Oct. 10, 2024), https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation#:~:text=These%20states%20are%20California%2C%20Connecticut,at%20the%20use%20of%20deepfakes.
[94] 2024 MS Senate Bill 2288.
[95] 2023 IL Senate Bill 382.
[96] *Id.*
[97] NCSL, *supra* note 92; Alabama Code Title 13A. Criminal Code § 13A-6-240.
[98] NCSL, *supra* note 92; 2023 NY Senate Bill 1042.

visual depiction of a minor engaging in a prohibited sexual act, or in a simulation of a prohibited sexual act, or any computer-generated child pornography."[99]

Each state also punishes these crimes differently. For example, Alabama's law described above classifies this offense as a Class A misdemeanor,[100] but South Dakota's law categorizes it as a Class 4 felony.[101]

States with laws penalizing deepfake pornography are examples of good progress, but addressing this issue solely at the state level presents several issues. As described above, state laws vary widely, with some states providing more protections to minors than others. States may define terms differently and impose different rules with different penalties. Furthermore, because online content can easily cross state lines, jurisdictional complications often arise.

It may seem unusual that more serious crimes, such as murder or rape, are typically handled only on the state level rather than under federal law.[102] However, these charges are "prosecuted as state crimes because the allegations within the charge violate state law," and only fall under federal jurisdiction in rare scenarios.[103] However, because online content can easily cross state lines, jurisdictional complications could easily arise with deepfake pornography, demonstrating a need for federal regulation.

2. Legal Treatment of and Issues with Similar Crimes

When states create their own laws, they are often modeled after their laws criminalizing revenge porn or child sexual abuse material.

a. Revenge Porn Laws

Revenge pornography—a tort commonly referred to as "revenge porn"—is "the intentional distribution of non-consensual porn [that] occurs when an ex-partner, hacker, or others post sexually explicit images of a person online without permission."[104] To date, forty-nine states, the District of Columbia, and Guam have statutes against revenge porn.[105]

---

[99] NCSL, *supra* note 92; 2024 SD Senate Bill 79.
[100] NCSL, *supra* note 92; Alabama Code Title 13A. Criminal Code § 13A-6-240.
[101] NCSL, *supra* note 92; 2024 SD Senate Bill 79.
[102] Neil Shouse, *7 Situations Where "Murder" Is a Federal Crime*, SHOUSE CAL. LAW GRP. (Mar. 7, 2024), https://www.shouselaw.com/ca/blog/murder/is-murder-a-federal-crime-7-ways-it-can-be/#:~:text=Many%20murder%20charges%20are%20prosecuted,is%20handled%20by%20federal%20prosecutors.
[103] For example, murder is considered a federal crime when the person murdered is "a federal judge or . . . federal law enforcement official," "an immediate family member of a federal law enforcement official," or "an elected or appointed federal official." Murder can also be considered a federal crime when "the killing is committed during a bank robbery," "takes place on federal property" or "aboard a ship at sea," or if the murder "was designed to influence a court case." Shouse, *supra* note 101.
[104] 1 Punitive Damages § 9.28.
[105] *Nonconsensual Distribution of Intimate Images*, CYBER C.R. INITIATIVE, https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images (last visited Nov. 16, 2024); Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479, 1501 (2020).

Using revenge porn laws as a framework to create new laws about deepfakes is a good starting point but poses several issues. First, each state has different revenge porn requirements and punishments. For example, some jurisdictions require "intent to cause emotional harm,"[106] others require "malicious intent when distributing the images,"[107] with others having no intent requirement at all.[108] The offense can also be classified as either a misdemeanor or a felony, depending on the jurisdiction.[109] If each state were to model their deepfake pornography laws after their existing revenge porn laws, the lack of consistency between states would cause problems, given the online nature of these crimes and their ability to transcend state lines.

Most importantly, revenge porn laws are based on principles of privacy law, but deepfakes may not be considered a violation of privacy. This is because the content may be easily recognizable as fake and the images may not be "taken seriously as an accurate depiction,"[110] as discussed above in Section II(A)(1). As one scholar notes, "[d]eepfakes are not fully 'real' in that they depict an act that never actually happened," and are rather based on photos that the victim has publicly posted online.[111] Thus, deepfakes are "not—legally speaking—a privacy violation."[112] Deepfakes, she notes, occupy a middle ground somewhere between real and fake, necessitating a new approach to account for this unique challenge.[113]

b. Child Sexual Abuse Material

For deepfake pornography depicting minors, some states have modeled their legislation after their existing laws for child sexual abuse material (CSAM). For example, Utah recently amended their CSAM laws to add that "[a]n actor is guilty of an offense if they 'commit the offense with the aid of a generative artificial intelligence' or 'intentionally promote[] or otherwise cause[] a generative artificial intelligence to commit the offense.'"[114]

Although deepfakes of minors can currently be prosecuted under CSAM statutes, this does not happen as frequently as it should due to various challenges. First, identifying perpetrators may be difficult. Although deepfake pornography creators sometimes reveal themselves to the victims—mostly in the case of teens creating deepfake porn of their friends—much of the time, the creators remain anonymous. Experts note that "[p]erpetrators can use various tools and techniques to mask their identities, making it challenging for law enforcement to track them down."[115]

Even when perpetrators can be identified, jurisdictional challenges may arise. As mentioned above, the online nature of these crimes makes it difficult for only one

---

[106] Katherine Gabriel, *Feminist Revenge: Seeking Justice for Victims of Nonconsensual Pornography Through "Revenge Porn" Reform*, 44 VT. L. REV. 849, 870 (2020).
[107] *Id.* at 869–70.
[108] *Id.* at 869.
[109] *Id.* at 868.
[110] Gieseke, *supra* note 104, at 1498.
[111] *Id.* at 1501–02.
[112] *Id.*
[113] *See id.*
[114] Lacey Johnson & John Feinauer, *Deepfakes, AI, and Intimate Images*, UTAH STATE LEG. 4 (Aug. 21, 2024), https://le.utah.gov/interim/2024/pdf/00003098.pdf.
[115] Samuel Dordulian, *Which States Have Passed Deepfake Laws?*, DORDULIAN LAW GRP. (Sept. 5, 2024), https://www.dlawgroup.com/states-have-passed-deepfake-porn-laws.

state's law to govern, as these cases may involve several states or even be distributed internationally.[116] Thus, it is essential that a federal law be enacted to create consistency across the board.

III. CONSTITUTIONAL FIRST AMENDMENT ISSUES

When creating laws, it is essential to understand constitutional barriers that must be complied with—most notably, First Amendment concerns—as well as their exceptions. The First Amendment states that "Congress shall make no law . . . abridging the freedom of speech."[117] Speech includes creating pictures and videos, so passing laws regulating deepfake pornography must fall under guidelines set forth by the Supreme Court to remain constitutional.

In order to pass a law that relates to deepfake pornography, the government can either "construct a narrowly tailored law that fits within the confines of the First Amendment," or they must "regulate deepfake pornography under existing categories of unprotected speech," such as obscenity or child pornography.[118]

A. Obscenity

Material is considered to be obscene, and thus unprotected by the First Amendment, when (1) "the average person . . . would find that the work, taken as a whole, appeals to the prurient interest"; (2) "the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law;" and (3) "the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."[119]

Obscenity could be applicable deepfake child pornography, but meeting its requirements can still be challenging. First, although many deepfakes would appeal to the prurient interest or be patently offensive, others may lack overtly sexual or offensive content yet still be embarrassing for the victim. For example, imposing someone's face onto a nude image from a medical textbook would not be sexual in nature but could still be damaging to the victim. Furthermore, even deepfake pornography—though likely not involving images of children—may be found to have artistic value, complicating obscenity classification.

B. Child Pornography

Child pornography is another unprotected category of speech. This category first began to be recognized in the late 1900s. In 1996, Congress passed the Child Pornography Prevention Act of 1996 (CPPA), banning "content that 'appears to be' child pornography but produced by means other than using real children, such as through the use of youthful-looking adult actors or computer-imaging technology."[120]

---

[116] *Id.*
[117] U.S. Const. amend. I.
[118] Emily Pascale, *Deeply Humanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse*, 73 SYRACUSE L. REV. 335, 342 (2023).
[119] Miller v. California, 413 U.S. 15, 24 (1973).
[120] Krista L. Baughman, *Will SCOTUS Reconsider Virtual Child Porn Laws in Light of Deepfake Culture?*, DAILY JOURNAL (Feb. 8, 2024), https://www.dailyjournal.com/articles/377089-will-scotus-reconsider-virtual-child-porn-laws-in-light-of-deepfake-culture.

In 2002, however, the Supreme Court introduced "limits on what can qualify as child pornography in *Ashcroft v. Free Speech Coalition*,"[121] and decided that the "appears to be" language used in the CPPA was overly broad, as it extended beyond obscenity and could ban content that had "redeeming artistic value," such as Shakespeare's *Romeo and Juliet*.[122] Thus, the Court "concluded that the statute was unconstitutional, explaining that virtual child pornography fell outside the constitutional category of child pornography."[123]

By doing so, the Court decided that "protecting *future* victims of child sex abuse [was not] a sufficient government interest," and clarified that "the harm of creation—that is, the sexual exploitation and abuse of children to produce child pornography—is the [basis] of . . . child pornography doctrine[,] . . . not what [the image] communicated."[124] However, the Court in *Ashcroft* left open the question of "whether images depicting real children, but created without sexual molestation or exploitation, are sufficiently similar to real child pornography to be exempt from First Amendment protection."[125]

Since then, "most courts have decided that images depicting real children, but created without sexual molestation or exploitation, still qualify as child pornography," and are thus included in this carve-out of the First Amendment.[126] Most notably, in 2009, the PROTECT Act was passed, defining "child pornography" to include "any computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct," or images that "ha[ve] been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."[127] However, scholars argue that this Act's provisions may be unconstitutional, as it "criminalizes all materials that are indistinguishable from child pornography," and may "grant[] prosecutors too much power to determine whom to charge."[128]

IV. POTENTIAL SOLUTIONS

Recognizing the challenges posed by deepfake pornography, lawmakers and companies alike have taken steps to address the issue, with some social media companies updating their privacy policies, and lawmakers proposing federal legislation.

A. Holding Tech Companies Liable

When determining liability, responsibility could fall on one of two parties: developers or deployers.[129] Developers are those who create the software, and

---

[121] Carissa Byrne Hessick, *The Expansion of Child Pornography Law*, 21 NEW CRIM. L. REV. 1, 3 (2019).
[122] Baughman, *supra* note 119; Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
[123] Hessick, *supra* note 120, at 3.
[124] *Id.* at 3–4.
[125] *Id.* at 4.
[126] *Id.*
[127] 18 U.S.C.S. § 2256.
[128] Rosalind E. Bell, *Reconciling the PROTECT Act with the First Amendment*, 87 NYU L. REV. 1878, 1903–04 (2012).
[129] Emory Odom, *Developers vs. Deployers: AI Leaders Demand Role Distinction in U.S. Legislation*, THE NAT'L CIO REV. (Oct. 18, 2024), https://nationalcioreview.com/articles-insights/technology/artificial-intelligence/developers-vs-deployers-ai-leaders-demand-role-distinction-

deployers are those who "apply these systems in the real world," such as using the software in a negative way to create or share deepfake pornography.[130] To hold tech companies liable, it is important to target the right actors, "avoiding unfair burdens on developers while ensuring deployers take responsibility for their usage."[131]

Although AI generation websites, categorized as developers, cannot be regulated due to First Amendment protections, some argue that tech companies themselves should play a part in resolving the issue, whether by having social media sites prohibit deepfake content from being posted or holding search engines accountable for allowing deepfake pornography sites to come up in search results. Such actions could effectively limit deployers in their ability to share harmful content.

1. Social Media Restrictions

Social media platforms may be able to help mitigate the problem through updating their policies on permissible content. For instance, X (formerly Twitter) updated its policies to prevent the spread of misinformation and other false content.[132] However, this approach has limitations: policies may too vaguely worded and may be abused to silence the wrong voices.[133] Additionally, "rely[ing] on private companies to police our societies" may not be very effective and perhaps holds the wrong parties accountable.[134]

2. Amending Search Engine Algorithms

Some even argue that search engine websites—in addition to AI generation websites or the social media platforms deepfakes are shared on—should play a part in the solution.[135] One writer notes that though Google tailors its search results in a positive way in some scenarios—such as displaying a suicide hotline as the first result when someone searches for ways to take their life—it fails to use similar precautions when someone searches for deepfake pornography.[136] While this would be a step in the right direction, encouraging search engines to prevent this kind of content from appearing in search results would not be sufficient to address the issue on its own.

3. Section 230 Immunity

Though passing legislation to hold these websites liable may sound like a good solution, this is not currently possible. Under Section 230 of the Communications Decency Act of 1996, social media platforms or other websites that host this content

---

in-u-s-legislation/#:~:text=For%20example%2C%20developers%20who%20build,responsibility%20for%20real%2Dworld%20implementations.

130 *Id.*

131 *Id.*

132 Arian Garshi, *Deepfakes in 2022: How Individual Non-Celebrities are Targeted*, MEDIUM (Oct. 17, 2022), https://ariangarshi.medium.com/deepfakes-in-2022-how-individual-non-celebrities-are-targeted-a7dab59cac3a; *Synthetic and Manipulated Media Policy*, X: HELP CTR. (Apr. 2023), https://help.x.com/en/rules-and-policies/manipulated-media.

133 Garshi, *supra* note 131.

134 *Id.*

135 Nicholas Kristof, *The Online Degradation of Women and Girls That We Meet With a Shrug*, WIRED (Mar. 23, 2024), https://www.nytimes.com/2024/03/23/opinion/deepfake-sex-videos.html.

136 *Id.*

cannot be held liable for allowing it to be spread.[137] This Act aims "to promote the continued development of the Internet," "to preserve the vibrant and competitive free market that presently exists for the Internet," and "to remove disincentives for the development and utilization of blocking and filtering technologies" that parents may use to limit children's access to harmful material.[138] There have been "dozens of [bipartisan] proposals to amend [or repeal] Section 230,"[139] so this obstacle may be eliminated in the future. However, for now, websites are effectively shielded from liability for third-party content its users post to its website.

Although many plaintiffs have challenged Section 230 immunity, only one has been successful thus far. This recent and notable case involved a ten-year-old girl who died doing the "Blackout Challenge," a TikTok trend that encouraged users "to asphyxiate themselves to the point of losing consciousness."[140] While the district court held that Section 230 shielded TikTok from liability, the court of appeals later reversed, clarifying that tech companies are "immunized only if they are sued for someone else's expressive activity or content (i.e., third-party speech), but they are not immunized if they are sued for their own expressive activity or content (i.e., first-party speech)."[141] Though the videos encouraging the challenge were created by third party users, the videos were pushed to the girl through TikTok's algorithm, which "decides on the third-party speech that will be included in or excluded from a compilation—and then organizes and presents the items" on each user's feed.[142] Thus, the appellate court concluded that the algorithm recommending the Blackout Challenge was TikTok's first-party speech and, therefore, was not protected under Section 230.[143]

However, this recent exception to Section 230 applies only to websites that use tailored algorithms to push content to users, meaning that websites that do not use such algorithms—like most sites that currently host deepfake pornography—remain protected.

B. Proposed Federal Criminal Legislation

No federal legislation has been passed yet to regulate deepfake pornography, but several acts have been proposed. Some federal proposed acts provide for civil remedies;[144] however, due to the challenges associated with relying on civil remedies

---

[137] 47 U.S.C.S. § 230.
[138] 47 U.S.C.S. § 230(b).
[139] *Section 230: A Brief Overview*, CONG. RSCH. SERV. (Feb. 2, 2024), https://crsreports.congress.gov/product/pdf/IF/IF12584.
[140] Gigen Mammoser, *Dangerous Social Media 'Blackout Challenge' Can Cause Brain Damage, Death in Less Than 5 Minutes*, HEALTHLINE (Sept. 9, 2024), https://www.healthline.com/health-news/tiktok-blackout-challenge.
[141] Anderson v. TikTok, Inc., 116 F.4th 180, 183 (3d Cir. 2024).
[142] *Id.* at 184.
[143] *Id.*
[144] The two federal proposed acts that provide victims with civil remedies are the DEFIANCE Act (short for Disrupt Explicit Forced Images and Non-Consensual Edits Act), which was introduced on January 30, 2024, and the No AI FRAUD Act (short for No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act), which was introduced on January 10, 2024.
The DEFIANCE Act allows "victims to sue if those who created the deepfakes knew, or 'recklessly disregarded' that the victim did not consent to its making." 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. To learn more about the DEFIANCE Act, see also Press Release, Rep. Ocasio-Cortez Leads Bipartisan, Bicameral Introduction of DEFIANCE Act to Combat Use of Non-

as discussed in Section II(A)(4), these proposals will not be discussed. Rather, this section will focus on the two federal proposed acts that provide victims with criminal remedies: the DEEP FAKES Accountability Act and the TAKE IT DOWN Act.

1. DEEP FAKES Accountability Act

The DEEP FAKES Accountability Act—short for Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability—was introduced on September 20, 2023, by Representative Yvette Clark (D-NY).[145] This Act seeks "[t]o protect national security against . . . deepfake technology and to provide legal recourse to victims of harmful deepfakes" by requiring a watermark or other textual descriptions on deepfake content.[146] It also requires verbal statements disclosing that the content has been altered if the content contains audio.[147]

This bill criminalizes "the production of [deepfakes] which do not comply with related watermark or disclosure requirements" as well as "the alteration of [deepfakes] to remove or meaningfully obscure such required disclosures," with penalties including "a fine, up to five years in prison, or both."[148]

However, this bill is unlikely to pass, as there are several issues with it. Although the Act would create a taskforce at the Department of Homeland Security to help combat deepfakes, it "would serve more of a research and reporting function" rather than provide a real enforcement mechanism to assist victims.[149] Others also note that the legislation would "burden legitimate users of [deepfake] technology and encumber courts with litigation due to its overbroad definition of 'deep fake.'"[150]

2. TAKE IT DOWN Act

The TAKE IT DOWN Act—an acronym for Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks—was introduced on June 18, 2024, by Senator Ted Cruz (R-TX).[151] As of this writing, this Act has passed the Senate.[152] This act "criminalize[s] the publication of non-

---

Consensual, Sexually-Explicit "Deepfake" Media, ALEXANDRIA OCASIO-CORTEZ (Mar. 7, 2024), https://ocasio-cortez.house.gov/media/press-releases/rep-ocasio-cortez-leads-bipartisan-bicameral-introduction-defiance-act-combat; S. 3696, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/senate-bill/3696.
The No AI Fraud Act "provides for individual property rights in likeness and voice." Evan Harris, *Deepfake Laws: A Comprehensive Overview*, PLURAL POLICY (May 23, 2024), https://pluralpolicy.com/blog/deepfake-laws. The Act seeks to protect "artists in the music industry[] who are encountering direct attacks to their intellectual property from abuse of [AI]," but this Act may also apply to deepfake pornography. Press Release, Salazar Introduces the No AI FRAUD Act, CONGRESSWOMAN MARIA ELVIRA SALAZAR (Jan. 10, 2024), https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act.

[145] DEEP FAKES Accountability Act, H.R. 3230, 116th Congress (2020).

[146] H.R. 3230.

[147] H.R. 3230; Lindsey Joost, *The Place for Illusions: Deepfake Technology and the Challenges of Regulating Unreality*, 33 U. FLA. J.L. & PUB. POL'Y 309, 330 (2023).

[148] H.R. 3230.

[149] Joost, *supra* note, at 330–31.

[150] Zachary Schapiro, *Deep Fakes Accountability Act: Overbroad and Ineffective*, B.C. INTELL. PROP. & TECH. FORUM 1, 1 (2020).

[151] TAKE IT DOWN Act, S. 4569, 188th Congress (2024).

[152] *Id.*

consensual intimate imagery (NCII), including AI-generated NCII (or 'deepfake pornography'), and require[s] social media and similar websites to have in place procedures to remove such content upon notification from a victim."[153] Although the Act only addresses NCIIs (including deepfake pornographic images) that are published—which may arguably be too narrow, as it may leave out unpublished deepfake pornography creations that may deserve penalty—the Act nonetheless is a step in the right direction toward effectively regulating deepfake pornography.

The Act permits victims to "submit a request for the . . . platform to remove [the] intimate visual depiction [of them]."[154] Victims must include in their request their signature (or a signature of their authorized representative), an "identification of the intimate visual depiction" of themselves, and "a brief statement that [they] ha[ve] a good faith belief that [the] intimate visual depiction . . . is not consensual, including any relevant information for the . . . platform to determine the intimate visual depiction was published without [their] consent."[155]

Upon receiving a removal request that meets the elements outlined above, a platform must "remove the intimate visual depiction and make reasonable efforts to remove any identical copies of such depiction as soon as possible, but not later than [forty-eight] hours after receiving [the] request."[156] By requiring websites to act on victim's requests within forty-eight hours, the bill seeks to ensure that "victims are protected from being retraumatized again and again" when this harmful content is posted.[157] If websites do not take the content down within the required time frame, their inaction will be "treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act,"[158] meaning that the website owners would be required to participate in a time-consuming process including an informal hearing.[159]

This bill also "criminalize[s] the publication of such content without the victim's consent"[160] and imposes fines, prison time (up to two years in prison for offenses involving adults and up to three years of imprisonment for offenses involving minors), or both for violations.[161]

Surprisingly, this bill has received no notable criticism, and many hope that it will be quickly enacted into law.[162] This bill addresses key issues in an effective way,

---

[153] Press Release, 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.
[154] S. 4569, Section 3(a)(1)(A).
[155] S. 4569, Section 3(a)(1)(B).
[156] S. 4569, Section 3(a)(3).
[157] S. 4569.
[158] S. 4569, Section 3(b)(1).
[159] 15 U.S.C. 57(a).
[160] *Considerations for Federal Right of Publicity as AI Advances*, LAW360: A LEXISNEXIS COMPANY (July 31, 2024).
[161] S. 4569.
[162] *Congress Must Pass TAKE IT DOWN Act*, AOL (July 6, 2024, 9:59 PM), https://www.aol.com/editorial-congress-must-pass-down-035900039.html.

"protect[ing] and empower[ing] victims of real and deepfake NCII, while protecting lawful speech."[163]

This legislation touches on several important points. First, it criminalizes not only the publication of NCII, including deepfake NCII, but also the threat to publish such content in interstate commerce when the intent is to "intimidat[e], coerc[e], extort[], or . . . distress" the victim.[164] Additionally, it "[p]rotects good faith efforts to assist victims" by including exceptions for law enforcement, legal and medical professionals, and others who intend to assist the victim.[165] Moreover, the bill is narrowly tailored to align with First Amendment guidelines, and criminalizes NCII without infringing on lawful speech, such as images used for "legitimate medical, scientific, or education purpose[s]."[166]

V. AMENDING THE TAKE IT DOWN ACT TO MANDATE SEX OFFENDER REGISTRATION

While the TAKE IT DOWN Act thoroughly addresses most issues, it could be improved with simple addition: clarifying that violators who publish deepfake pornography of children should also be categorized as Tier I sex offenders, which carries with it mandatory sex offender registration for ten to fifteen years.

A. Sex Offender Registries

Sex offender registries are meant to help law enforcement "monitor[] and track[] sex offenders following their release into the community" and to alert the public of their existence.[167] Registered sex offenders must appear in person at regular intervals "to take a current photograph and verify . . . where they live, work[,] and go to school."[168] Sex offender registries are managed at the state level, as sex offenders must report to state authorities to update their registration, but there is still a large federal component to them. While there is no federal sex offender registry, the Sex Offender Registration And Notification Act (SORNA)—a federal law—requires "every state to participate in the Dru Sjodin National Sex Offender Public Website, which pulls information from all the states into one searchable database,"[169] allowing people from every state to easily identify potential predators.

---

[163] *The TAKE IT DOWN Act: Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Network*, 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 Nov. 17, 2024).
[164] S. 4569; TODD YOUNG, *supra* note 158.
[165] TODD YOUNG, *supra* note 158.
[166] *Id.*
[167] *See Sex Offender Registration And Notification Act (SORNA)*, U.S. DEP'T OF JUST. (Aug. 11, 2023), https://www.justice.gov/criminal/criminal-ceos/sex-offender-registration-and-notification-act-sorna#:~:text=Sex%20Offender%20Registration%20And%20Notification%20Act%20(SORNA),-MENU%20Subject%20Areas.
[168] *Frequently Asked Questions*, SMART, https://smart.ojp.gov/faqs#2-0 (last visited Nov. 17, 2024).
[169] Rebecca Pirius, *State and Federal Sex Offender Registration Laws*, CRIM. DEF. LAW. (Oct. 18, 2024), https://www.criminaldefenselawyer.com/resources/state-sex-offender-registration.htm.

There are three tiers of sex offender classifications: Tier I, Tier II, and Tier III.[170] Each category is associated with different crimes and comes with different penalties and registration requirements.[171]

Tier I is reserved for sex offenders who do not meet the requirements for Tier II or III,[172] and is generally reserved for misdemeanor sex crimes,[173] which may include "[h]aving or receiving child pornography[,] . . . [v]ideo voyeurism of a minor[,] . . . [or] [t]ransmitting information about a minor to further criminal sexual misconduct."[174] These offenders are only required to verify their registration information annually and typically must remain on the sex offender registry for a minimum of fifteen years.[175] However, if these offenders maintain a clean record, their registration period may be reduced to ten years.[176]

Tier II sex offenders are those who have committed "less serious felony sex crimes,"[177] including crimes that are "punishable by imprisonment for more than one year."[178] These crimes may include sex trafficking, coercion and enticement, transportation with intent to engage in criminal sexual activity, or abusive sexual contact.[179] Tier II offenders must verify their registration information every six months and remain on the registry for twenty-five years.[180]

Tier III is reserved for sex offenders who have committed serious felony sex crimes, such as kidnapping by a non-parent, aggravated sexual abuse, sexual abuse, or abusive sexual contact against a minor younger than thirteen years old.[181] These offenders must verify their registration information every three months and are required to remain on the sex offender registry for life.[182]

Because the TAKE IT DOWN Act already criminalizes deepfake pornography to be treated similarly to genuine pornography, offenders should be placed in the Tier I category, alongside those convicted of pornography-related offenses. Classifying those who create deepfake pornography of minors as Tier I offenders is also most appropriate because deepfake pornography, while serious, is not as egregious as crimes like sex trafficking (a Tier II offense) or aggravated sexual abuse (a Tier III offense). This would impose a lower burden on the perpetrators in comparison to other

---

[170] 34 U.S.C. § 20911.
[171] *See* 34 U.S.C. § 20911; SMART, *supra* note 163.
[172] 34 U.S.C. § 20911(2).
[173] John Devendorf, *An Overview of Tiers for Convicted Sex Offenders*, LAWINFO (Mar. 12, 2024), https://www.lawinfo.com/resources/sex-crime/sex-offender-tiers.html.
[174] Tammy Cohen, *What Violations Can Land You on a Sex Offender Registry?*, INFOMART (Apr. 29, 2016), https://www.infomart-usa.com/blog/violations-can-land-sex-offender-registry/#:~:text=Offenses%20that%20Can%20Lead%20to%20Sex%20Offender%20Registration&text=Offenses%20often%20fall%20into%20categories,Attempted%20offenses%20are%20also%20prosecuted.
[175] SMART, *supra* note 163.
[176] *Id.*
[177] Devendorf, *supra* note 167.
[178] 34 U.S.C. § 20911(3).
[179] *Id.*
[180] SMART, *supra* note 163.
[181] 34 U.S.C. § 20911(4).
[182] SMART, *supra* note 163.

classifications, as they would only need to verify their information annually and can be on the registry for as little as ten years.

To accomplish this, lawmakers would only need to amend the existing TAKE IT DOWN Act rather than draft an entirely new bill. While this may seem like a large undertaking, only Section (3)(B), which contains penalties for offenses involving minors, would need to be revised. Because statutory language outlining the registration requirements for sex offenders already exists,[183] and because the Act defers to other sections of the United States Code in its language,[184] lawmakers could follow that same framework and simply refer to that section of the U.S. Code rather than redefining the terms themselves.

Thus, the revised section could state something as simple as the following (modifications italicized): "Any person who violates paragraph (2)(B) shall be fined under title 18, United States Code, imprisoned not more than 3 years, or both, *and shall comply with registration requirements for Tier I sex offenders pursuant to title 34, United States Code, Sections 20911–20931*."

B. Policy Considerations

Requiring sex offender registration would not only hold perpetrators accountable but also inform communities of dangerous individuals around them. For social media users wanting to protect their images, this awareness could encourage them to make their accounts private or, for already private users, to be more cautious about accepting new follow or friend requests. Additionally, it would allow parents identify members of their communities who may be dangerous, whether that be physically or online.

This approach would hold adults responsible for their actions while offering grace to minors who may not have thought through the consequences of creating or sharing a deepfake of a peer. Under SORNA, minors are only required to register as juvenile sex offenders if they have committed "particularly serious sexual assault crimes," typically crimes that are "comparable to or more serious than aggravated sexual abuse,"[185] meaning that minors who create or distribute deepfake pornography—assuming they have not been convicted of aggravated sexual abuse in the past—would be able to learn from their mistakes without having to endure the challenges that come with carrying a long-lasting mark on their record.

Mandating sex offender registration may seem like a harsh approach, as most criminals would rather serve more time than have a mark on their record that may put restrictions on where they can live or work.[186] However, even offenses as inconsequential as urinating in public can land someone on the sex offender registry, so deepfake child pornography offenses should warrant the same consequence.[187] If

---

[183] 34 U.S.C. § 20913.
[184] S. 4569.
[185] SMART, *supra* note 163.
[186] Rachel Marshall, *I'm a Public Defender. My Clients Would Rather Go to Jail Than Register as Sex Offenders*, VOX (July 5, 2016, 6:00 AM), https://www.vox.com/2016/7/5/12059448/sex-offender-registry.
[187] Tammy Cohen, *What Violations Can Land You on a Sex Offender Registry?*, INFOMART (Apr. 29, 2016), https://www.infomart-usa.com/blog/violations-can-land-sex-offender-

the public can be made aware of those who may indecently expose themselves—which arguably poses little to no threat to others—they should also be informed of predators who may exploit images of minors. Additionally, given that many offenders would prefer prison time over registration,[188] stating clearly that mandatory registration would be a consequence could potentially deter people from creating or publishing deepfake pornography in the first place.

Finally, because deepfake pornography of minors is treated the same as authentic child pornography under the TAKE IT DOWN Act, some states may already require sex offender registration for this offense. Amending the Act to include mandatory registration would ensure consistency across the board.

CONCLUSION

Deepfake pornography—especially that depicting minors—is a serious issue that demands a serious solution. Mandating sex offender registration for those who possess or publish deepfake pornography of minors would alert communities of people who are dangerous around them, notifying parents to guard their children and images of them, while also protecting minors who create deepfake pornography of their peers, as they would not be required to register. Adding this brief provision to the TAKE IT DOWN Act—a bill already poised for success—rather than drafting an entirely new bill would increase its likelihood of becoming enacted law while avoiding logistical issues. By raising awareness of and penalizing individuals who may use others' images in a violating way, lawmakers can deter individuals from creating deepfake pornography, hold offenders accountable for their actions, and most importantly, empower individuals to protect themselves.

registry/#:~:text=Offenses%20that%20Can%20Lead%20to%20Sex%20Offender%20Registration&text=Offenses%20often%20fall%20into%20categories,Attempted%20offenses%20are%20also%20prosecuted.

[188] Marshall, *supra* note 181.