LET'S BE REALISTIC: CRAFTING AN EFFECTIVE LEGAL REMEDY FOR VICTIMS OF DEEPFAKE PORNOGRAPHY

Niki Saenz*

Generative artificial intelligence has created a new frontier of sexual violence worldwide: deepfake pornography. What once required technological expertise and sophisticated software is now in the hands of the general public, creating victims of all ages, races, genders, and sexual orientations. By creating false media depicting victims, mainly women, in fabricated sexual acts, perpetrators subject victims to mental, emotional, reputational, and even physical harm. Traditional legal avenues, such as tort law, intellectual property law, and state nonconsensual pornography statutes, are not equipped to handle the new technology and, therefore, only provide imperfect solutions for victims. Among the few state laws on deepfake pornography, protections and requirements for victims vary depending on where they are in the country. This Note argues that Congress has the power to sidestep legal barriers faced by state governments and victims alike. With nonconsensual pornography laws and state deepfake pornography laws to inform it, Congress should pass federal criminal legislation that applies clearly, uniformly, and efficiently across the country. Such legislation will provide past, current, and future victims of deepfake pornography with the justice they deserve.

TABLE OF CONTENTS

---

* JD Candidate, University of Arizona James E. Rogers College of Law, 2025. This Note would not be possible without the village of people standing behind me. To the *Arizona Law Review* team that shaped this Note, thank you for all your hard work. To my advisor, Professor Andrew Woods, thank you for your insight and guidance throughout this process. To my wonderful family, friends, and partner, thank you for all the hours you spent listening to me nerd-out about this issue, and thank you for your endless love and support.

INTRODUCTION

More than 45 million views, 24,000 reposts, and hundreds of thousands of likes and retweets later, deepfake pornography targeting Taylor Swift was removed from X.[1] Of course, these numbers represent only the original post of the sexually explicit material, and duplicates have since spread to different accounts, platforms, and other dark corners of the internet.[2] Luckily for Swift—the billionaire, 2023 Time Person of the Year, and 14-time Grammy Award winner—the post was removed within 17 hours, and "Swifties"[3] flooded hashtags with real media of Swift to hide the explicit fakes.[4] Even for Swift, however, the damage is far from over. Like thousands of other women—the non-famous, celebrities, and political officials

1. Jess Weatherbed, *Trolls Have Flooded X with Graphic Taylor Swift AI Fakes*, THE VERGE (Jan. 25, 2024, 9:04 AM), https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending [https://perma.cc/25N9-M56Y].

2. *Id.*

3. *Swiftie*, Dictionary.com, https://www.dictionary.com/e/pop-culture/swiftie/ [https://perma.cc/P66R-CF8K] (last visited Jun. 19, 2024).

4. Weatherbed, *supra* note 1; Alexandra del Rosario, *Taylor Swift Makes Even More History as Time Magazine's 2023 Person of the Year*, L.A. TIMES (Dec. 6, 2023), https://www.latimes.com/entertainment-arts/music/story/2023-12-06/taylor-swift-time-person-of-the-year-2023-makes-history [https://perma.cc/TS75-FBFN].

alike—there may be no legal recourse to recover for the latest form of sexual exploitation and technological abuse. If one of the most powerful women in the world cannot find legal recourse for the harms she has faced from deepfake pornography, what hope is there for anyone else?

In a world where generative artificial intelligence ("AI") is available to anyone with internet access, users can sexually exploit others, mainly women, through AI-generated "deepfake" pornography. Although deepfake pornography has been around for years, the recent explosion of generative AI has made this harmful technology available to unsophisticated users and, therefore, has made its harm reach further than it has before. Generative AI at large has captured the attention of the Biden Administration and the European Union, both of which are attempting to draft frameworks to regulate the technology.[5]

In a time when legislatures may be rushing to pass legislation on deepfake pornography, this Note urges lawmakers to learn from the advantages and downfalls of current legislation to craft the most effective and just law possible for victims of deepfake pornography. This Note proceeds as follows: Part I will provide background on deepfake pornography, from both a technological perspective and from traditional notions of sexual privacy. Part II will identify existing paths to legal recourse for victims of nonconsensual deepfake pornography, compare current state laws, and discuss heuristics from laws on nonconsensual pornography. Finally, Part III will suggest how to best model federal legislation to provide comprehensive recourse to victims. A brief conclusion follows.

I. BACKGROUND

A. Understanding Generative AI

Generative AI refers to artificial intelligence programs that use a large body of data, such as text, images, or other data, to "create, at the request of users, new versions of text, images, or predicted data."[6] Generative AI, although recently under the scrutiny of the public, has been used in technology, education, and creative industries for years.[7] Film producers, for example, can use generative AI to make films with deceased actors.[8] ALS patients and others who suffer from paralysis can

---

5. *See* Exec. Order No. 14,110, 88 Fed. Reg. 210 (Oct. 30, 2023); EUR. PARL. DOC. (COR01) (2024), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf [https://perma.cc/QZD6-4PHU]. The scope of the analysis in this Note will focus on common and statutory law in the United States. Further research is needed to analyze international laws on generative AI, their effect on online platforms operating in the United States or otherwise, and their effect on victims of deepfake pornography.

6. Jim Euchner, *Generative AI*, 66 RSCH. TECH. MGMT. 71, 71 (2023).

7. *Id.*; Moncarol Y. Wang, *Don't Believe Your Eyes: Fighting Deepfaked Nonconsensual Pornography with Tort Law*, 2022 U. CHI. LEGAL F. 415, 418 (2022).

8. Wang, *supra* note 7, at 418. The use of generative AI in film, while permitted, is hotly contested. During the 2023 strike, SAG-AFTRA fought, in part, to restrict the use of AI in film. Despite this, the final negotiation does not prohibit the use of AI and "does relatively little to stop studios from training on actors' performances to create 'synthetic' performers." Gene Maddaus, *SAG-AFTRA Board Members Explain 'No' Votes: 'There Should Be No AI'*, VARIETY (Nov. 14, 2023, 4:07 PM), https://variety.com/2023/biz/news/

use generative AI to create voice avatars that allow the patients to speak with their own voices.[9] AI-generated depictions of historical figures have been used to enrich museum exhibits[10] and children's educational television shows.[11]

However, much of the recent public discourse surrounds the use of large language models, such as ChatGPT, and image-generation models, such as DALL-E.[12] These tools put generative AI in the hands of everyday people, not just those with technological expertise. They rely on "deep learning," a subfield of artificial intelligence that uses large amounts of data to repetitively carry out tasks, adjusting its processes each time to enhance the overall outcome.[13] In other words, like humans, these programs learn from experience.[14] Deep learning results in text, audio, photographs, and videos that appear astonishingly legitimate but are fabricated by artificial intelligence.[15]

B. Understanding Deepfakes

"Deepfakes" are any type of generated or manipulated digital media, such as images, videos, audio, or text, created using artificial intelligence and deep-learning algorithms.[16] For the purposes of this Note, the focus will be on deepfake images and videos. These types of deepfakes are created by "training" an AI program—providing it with reference pictures and videos to analyze.[17] First, the AI program extracts the original picture from the original frame.[18] Then, the extracted picture is used as deep-learning input as the algorithm generates an exact match for the original picture.[19] Once adequately trained, the program will recreate the original image and then "swap" it into the target media.[20] These AI programs can "overlay face images, create facial motions, switch faces, maneuver facial expressions, produce faces, and synthesize the speech of a target individual onto a video of a spokesperson," essentially morphing an individual into the role of the person in the

---

sag-aftra-ai-artificial-intelligence-board-no-votes-1235790853/ [https://perma.cc/7HBP-2RQY].

9. Wang, *supra* note 7, at 419.

10. *Id.* at 418; *see also* Dami Lee, *Deepfake Salvador Dalí Takes Selfies with Museum Visitors*, THE VERGE (May 10, 2019), https://www.theverge.com/2019/5/10/18540953/salvador-dalilives-deepfake-museum [https://perma.cc/C89D-NRM8] (quoting Dalí in saying, "I believe in general in death, but in the death of Dali, absolutely not").

11. Wang, *supra* note 7, at 418.

12. Euchner, *supra* note 6, at 71.

13. LOVELEEN GAUR ET AL., INTRODUCTION TO DEEPFAKE TECHNOLOGIES 1 (2023).

14. *Id.*

15. *Id.* at 2.

16. *Id.*; *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*, FBI (June 5, 2023), https://www.ic3.gov/Media/Y2023/PSA230605#fna [https://perma.cc/P472-WY4G].

17. Alexandra Arko & Mark Rasch, *Nudify Me: The Legal Implications of AI-Generated Revenge Porn*, JD SUPRA (Feb. 16, 2023), https://www.jdsupra.com/legalnews/nudify-me-the-legal-implications-of-ai-2348218/ [https://perma.cc/4RJ4-JM4Y].

18. GAUR ET AL., *supra* note 13, at 4.

19. *Id.*

20. Arko & Rasch, *supra* note 17; GAUR ET AL., *supra* note 13, at 2.

source.[21] Deepfakes can be used in virtually any context, from viral social media filters[22] to depictions of political figures.[23] Whether the intent is innocent or malicious, at the heart of deepfakes is a goal to create false media that depicts people doing or saying things they never did.[24]

C. Understanding Deepfake Pornography

Deepfake pornography, therefore, is pornographic media created using AI that depicts people in lewd sexual acts that they themselves did not participate in.[25] The harm from deepfake pornography stems from two broad aspects of deepfakes: misperception and availability.[26]

Misperception occurs because deepfakes can depict false media with increasing accuracy.[27] The human brain is designed to believe what it witnesses itself.[28] As a result, victims of deepfake pornography are subject to immense social and reputational harm from the misrepresentations of deepfake pornographic videos.[29] Moreover, the presence of nonconsensual deepfake pornography creates mental and emotional harm for victims, as well as a threat for physical harm.[30]

Availability becomes an issue because with new easy-to-use apps, creating a deceiving deepfake does not require technical expertise.[31] As tools and technologies develop, they become accessible to everyday users.[32] Furthermore, the AI programs needed to create deepfake pornography do not necessarily need to be trained on sexual or lewd media references of the victim.[33] Rather, these programs can be trained only using photos of the victim's face.[34] Such photos can be sourced from websites, social media, or camera rolls. In fact, there are open-source tools that download all images of an individual from her social media accounts to create the reference materials an AI program needs to create deepfake media.[35]

---

21. GAUR ET AL., *supra* note 13, at 2.

22. Bernard Marr, *Picture Perfect: The Hidden Consequences of AI Beauty Filters*, FORBES (June 9, 2023, 02:06 AM), https://www.forbes.com/sites/bernardmarr/2023/06/09/picture-perfect-the-hidden-consequences-of-ai-beauty-filters/?sh=47f04d577d5d [https://perma.cc/F485-74TQ].

23. Alyssa Ivancevich, *Deepfake Reckoning: Adapting Modern First Amendment Doctrine to Protect Against the Threat Posed to Democracy*, 49 HASTINGS CONST. L.Q. 61, 63 (2022).

24. *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*, *supra* note 16; GAUR ET AL., *supra* note 13, at 2.

25. *See* GAUR ET AL., *supra* note 13, at 2.

26. *Id.* at 4.

27. *Id.*

28. *Id.*

29. Jared de Guzman, *Saving Face: Lessons from the DMCA for Combating Deepfake Pornography*, 58 GONZ. L. REV. 109, 112 (2023).

30. *Id.*

31. GAUR ET AL., *supra* note 13, at 4; de Guzman, *supra* note 29, at 111–12.

32. GAUR ET AL., *supra* note 13, at 4; de Guzman, *supra* note 29, at 111–12.

33. *See* Wang, *supra* note 7, at 420.

34. *See id.*

35. *See id.* This Note does not include specific examples of these tools to avoid increased exposure and publicity to such harmful technologies.

As deepfake technology becomes more accessible to unsophisticated users, those at risk of becoming victims of deepfake pornography are expanding from celebrities and public figures to average people.[36] Anyone can be a victim of deepfake pornography, regardless of age, gender, race, or sexual orientation.[37] Nonetheless, nonconsensual deepfake pornography is mainly a violence-against-women issue.[38] From 2018 to 2021, it is estimated that up to 95% of deepfake videos online were nonconsensual deepfake porn.[39] Of those, about 90% depicted women.[40] The amount of pornographic deepfakes online is growing exponentially.[41] In the first nine months of 2023, there was a 54% surge in deepfake pornography, with 113,000 videos uploaded to the leading 35 websites, compared to 73,000 for the entire year of 2022.[42] This is only a snapshot of the problem—it does not encompass deepfake photos, deepfake videos posted to social media, or those shared privately.[43] In other words, technology "gave the world powerful AI tools, and the world made porn with them."[44]

D. Nonconsensual Pornography and Sexual Privacy

The discourse about deepfake pornography begins with a discussion of nonconsensual pornography, otherwise known as "revenge porn." Importantly, the term "revenge porn" is discouraged because it is misleading and undermines the harmful effects of nonconsensual pornography.[45] Often, nonconsensual pornography is perpetrated not out of vindictiveness, but out of motives such as

---

36. Brian Feldman, *MacArthur Genius Danielle Citron on Deepfakes and the Representative Katie Hill Scandal*, N.Y. MAG. (Oct. 31, 2019), https://nymag.com/intelligencer/2019/10/danielle-citron-on-the-danger-of-deepfakes-and-revenge-porn.html [https://perma.cc/G5QD-EYL2].

37. *Cf.* Anne Pechenik Gieseke, *"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479, 1502 (2020) ("[T]he number of potential victims of deepfake pornography is effectively unlimited. This number includes 'anyone whose image has been captured digitally' and posted on the internet.").

38. de Guzman, *supra* note 29, at 111–12.

39. Karen Hao, *Deepfake Porn is Ruining Women's Lives. Now the Law May Finally Ban It.*, MIT TECH. REV. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/ [https://perma.cc/A8UN-7TDN].

40. *Id.* Some sources report even higher rates of nonconsensual deepfake pornography that depicts women. Feldman, *supra* note 36 ("98% of deep fakes that are appearing online are deep fake sex videos. And 99% of deep fake sex videos involve women . . . .").

41. Matt Burgess, *Deepfake Porn Is Out of Control*, WIRED (Oct. 16, 2023), https://www.wired.com/story/deepfake-porn-is-out-of-control/ [https://perma.cc/XJ5D-UKUP].

42. *Id.*

43. *Id.*

44. Danielle S. Van Lier, *The People vs. Deepfakes: California AB 1903 Provides Criminal Charges for Deepfakes Activity to Guard Against Falsified Defaming Celebrity Online Content*, 43 L.A. LAW. 16, 18 (2020).

45. Wang, *supra* note 7, at 421; MARY ANNE FRANKS, CYBER C.R. INITIATIVE, DRAFTING AN EFFECTIVE "REVENGE PORN" LAW: A GUIDE FOR LEGISLATORS 2 (2021), https://cybercivilrights.org/wp-content/uploads/2021/10/Guide-for-Legislators-10.21.pdf [https://perma.cc/D6ET-GXDU].

greed, voyeurism, and self-aggrandizement.[46] Therefore, this Note will use the term "nonconsensual pornography."

Nonconsensual pornography is "the distribution of sexually graphic images of individuals without their consent."[47] Media used for nonconsensual pornography can be exchanged voluntarily with another person in the context of a private relationship or obtained involuntarily through hacking and nonconsensual documentation of sexual acts.[48] The modern trend involves perpetrators uploading nonconsensual pornography online to social media sites or nonconsensual-pornography-specific websites.[49] However, "low-tech" forms of nonconsensual pornography still exist, such as printed images and DVDs.[50]

Nonconsensual pornography is also a violence-against-women issue.[51] Women are more likely to be victims, and men are more likely to be perpetrators.[52] Beyond the immense mental, social, and reputational harm that nonconsensual pornography causes, women also experience threats, harassment, and violence as a result of nonconsensual pornography.[53] Further, nonconsensual pornography has a chilling effect on women's speech, expression, and professional aspirations.[54] Experience with or threats of nonconsensual pornography deter women from participating in important spheres of modern life such as work,[55] school, social media, and personal relationships.[56]

Deepfake pornography is nonconsensual pornography in the age of generative AI.[57] Nonconsensual pornography differs from deepfake pornography in that the media is taken by or of the victim's actual person, rather than an AI-generated depiction of the victim.[58] Although most states and the federal government have passed laws on nonconsensual pornography,[59] few jurisdictions have been successful in passing or adapting laws on nonconsensual pornography to include nonconsensual deepfake pornography.[60]

---

46. Wang, *supra* note 7, at 421; FRANKS, *supra* note 45, at 2.
47. FRANKS, *supra* note 45, at 1.
48. *Id.*
49. *Id.* at 4–5.
50. *Id.* at 12.
51. *Id.* at 3.
52. *Id.*
53. *Id.* at 3–4.
54. *Id.* at 4.
55. In fact, women are often deterred from pursuing vocations such as politics and journalism because of the chilling effects of nonconsensual pornography. *Id.*
56. *Id.*
57. *See* Wang, *supra* note 7, at 422.
58. *Id.*
59. FRANKS, *supra* note 45, at 5 ("As of October 2021, forty-eight state legislatures, the District of Columbia, the territory of Guam, and the Uniform Code of Military Justice have recognized the devastating impact of this form of privacy violation through criminal statutes."); 15 U.S.C. § 6851.
60. Emily Pascale, *Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and The Path to Legal Recourse*, 73 SYRACUSE L. REV. 335, 342–43 (2023).

Both nonconsensual pornography and deepfake pornography fit into a larger discussion of sexual privacy.[61] Introduced by Danielle Keats Citron, sexual privacy refers to governing the management and boundaries of one's intimate life.[62] Sexual privacy captures many things: expectations concerning the seclusion of physical spaces where people have sex and undress; assumptions about the concealment of naked body parts in varied contexts; the presumed confidentiality of communications about intimate activities; and the expectation of autonomy in decisions to share one's nude body with others, among other ideas.[63]

Sexual privacy lives at the heart of Samuel Warren and Louis Brandeis's "right to be let alone," which argues that individuals should control how much others know about their "domestic circle."[64] Warren and Brandeis argued that a right to privacy would protect an individual's ability to develop their "inviolate personality."[65] Citron expands on this by arguing that human dignity requires that "individuals should determine the arc of their intimate lives."[66] Although nonconsensual pornography and deepfake pornography are different mechanisms with different paths to legal recourse, both disrupt the arc of victims' intimate lives. In doing so, victims, often women, are left with immense mental, emotional, reputational, occupational, and even physical harm.[67]

II. CURRENT LEGAL REMEDIES

There is no one-size-fits-all legal remedy for victims of deepfake pornography. The paths to legal recourse vary by jurisdiction, as well as the nature and circumstances of the pornographic media itself. Currently, the landscape of legal remedies for victims is a patchwork that may be available in some cases but not others. In the vast majority of cases, victims have no legal remedy.[68] This Part will discuss current legal remedies available at common law, as well as state statutes on deepfake pornography and nonconsensual pornography.

A. Section 230 and the Problem of Identifying a Defendant

One issue with assessing liability for deepfake pornography is deciding who to hold liable in the first place. While some obvious defendant choices would be the AI platforms where the content is created or the web platforms where the content is distributed, a large shield protects such platforms from liability: Section 230 of the Communications Decency Act ("Section 230").[69]

Section 230, passed in 1996, provides immunity from legal liability for platforms in two ways. First, it says that an "interactive computer service" cannot

61. Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1878 (2019).
62. *Id.* at 1880.
63. *Id.* at 1880–81.
64. *Id.* at 1885.
65. *Id.* at 1885–86.
66. *Id.* at 1886.
67. *Id.* at 1926–27.
68. Hao, *supra* note 39.
69. 47 U.S.C. § 230(c).

be treated as the publisher or speaker of third-party content.[70] In other words, Section 230 protects platforms from liability for user actions and speech on the platform. Second, it ensures that platforms are not held liable for voluntarily acting to restrict access to objectionable material.[71] This means that a web platform cannot be held liable for any good-faith attempts to remove harmful material from its site.[72] Simply put, Section 230 protects platforms from liability for users' speech.[73]

Since its inception, courts have construed Section 230 broadly.[74] Initially, Section 230 was adopted in response to *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[75] which held that an internet service provider's editorial control over the content on its site made it equivalent to a traditional publisher.[76] Congress passed Section 230 to supersede this ruling, fearing that it would discourage investments in the internet at its infant stage.[77] In doing so, the law evolved to treat service providers as nothing more than "empty news racks for users to freely populate with content."[78] *Zeran v. America Online, Inc.*[79] expanded Section 230's protections by barring liability for distributing harmful material as well.[80] The *Zeran* court reasoned that in Section 230, the use of the term "publisher" includes traditional publishers as well as distributors.[81] This holding has been applied by every federal circuit court and numerous state courts.[82]

Section 230's protections, while broad, are not absolute.[83] Section 230(e) outlines five exceptions to the immunity created by Section 230: (1) federal criminal law, (2) intellectual property law, (3) state laws "consistent" with Section 230, (4) communications privacy laws, and (5) sex trafficking laws.[84]

The first three exceptions are particularly relevant in a discussion of deepfake pornography. The first exception provides that any defendant in a federal criminal prosecution cannot claim immunity under Section 230.[85] This exception is

---

70. Casey Newton, *Everything You Need to Know About Section 230*, THE VERGE (Dec. 29, 2020, 2:50 PM), https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation [https://perma.cc/LM8Q-RKKB].

71. 47 U.S.C. § 230(c)(2); VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 3 (2021), https://crsreports.congress.gov/product/pdf/R/R46751 [https://perma.cc/PG4J-U4QC].

72. 47 U.S.C § 230(c)(2); BRANNON & HOLMES, *supra* note 71, at 3.

73. *See Section 230*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/NGL6-4NKX] (last visited Nov. 27, 2023).

74. 47 U.S.C. § 230(c)(2); *Section 230: An Overview*, *supra* note 71, at 10.

75. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

76. *Id.* at *4; BRANNON & HOLMES, *supra* note 71, at 10.

77. Wang, *supra* note 7, at 432.

78. *Id.*

79. 129 F.3d 327 (4th Cir. 1997).

80. *Id.* at 332; BRANNON & HOLMES, *supra* note 71, at 11.

81. *Zeran*, 129 F.3d at 332; BRANNON & HOLMES, *supra* note 71, at 11.

82. BRANNON & HOLMES, *supra* note 71, at 11.

83. 47 U.S.C. § 230(e); *Section 230*, *supra* note 73.

84. 47 U.S.C. § 230(e).

85. BRANNON & HOLMES, *supra* note 71, at 27.

limited to criminal prosecution and does not allow civil lawsuits based on violations of federal criminal laws.[86]

The second exception provides that defendants do not have Section 230 immunity for violations of "any law pertaining to intellectual property."[87] Since "intellectual property" is undefined, circuits interpret the term differently.[88] The Ninth Circuit, for example, only applies the exception to "claims pertaining to an established intellectual property right under federal law, like those inherent in a patent, copyright, or trademark."[89] Circuits are also split on whether the term includes state intellectual property laws, such as the right of publicity.[90] The Third Circuit, for example, interprets "any law" to mean that the exception includes state intellectual property rights.[91] The Ninth Circuit, on the other hand, only recognizes federal intellectual property rights as part of the exception.[92]

The third exception provides that Section 230 will not "prevent any State from enforcing any State law that is consistent with this section."[93] Congress did not define how a state law would be "consistent" with Section 230, but courts generally look "to whether the [state] law would violate Section 230(c)(1) by treating service providers or users as the publisher of another person's content."[94] If a state law is inconsistent with Section 230, regardless of whether it is a civil or criminal provision, it is preempted by Section 230.[95]

Proponents of Section 230 claim that "[t]he free and open internet as we know it" would not exist without the legislation.[96] By passing Section 230, Congress intended to promote the growth of the internet by protecting service providers from liability for user-posted harmful material.[97] Without Section 230's protections, proponents argue, many online service providers would intensively filter and censor user speech, and others would be chilled to the point of not being able to host user content at all.[98] In its infancy, the internet needed this protection to grow into the landscape of diverse discourse and communities we know it as today.[99]

However, critics argue that "the Internet has outgrown its swaddling clothes and no longer needs to be so gently coddled."[100] As the internet has grown,

---

86. *Id.*
87. 47 U.S.C. § 230(e)(2); BRANNON & HOLMES, *supra* note 71, at 27.
88. BRANNON & HOLMES, *supra* note 71, at 27–28.
89. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1053 (9th Cir. 2019).
90. BRANNON & HOLMES, *supra* note 71, at 28.
91. *Id.* at 28–29.
92. *Id.* at 29.
93. 47 U.S.C. § 230(e)(3).
94. BRANNON & HOLMES, *supra* note 71, at 29.
95. *Id.* at 27.
96. *Section 230*, *supra* note 73.
97. 47 U.S.C. § 230(a)–(b).
98. *Section 230*, *supra* note 73.
99. *See id.*
100. Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1175 n.39 (9th Cir. 2008).

online service providers no longer need such sweeping protections.[101] With such broad-spanning immunity for platforms, Section 230 makes it nearly impossible to succeed in claims brought against them, despite their shared responsibility in perpetrating the creation and distribution of content-based harms, such as those caused by deepfake pornography.[102] Instead, victims are forced to name the "publisher" of the harm as a defendant.[103] In cases where the publisher of the content is anonymous or hiding behind an IP address, victims may have no chance of holding anyone responsible for the harms they have faced.[104]

With the explosion of public-facing generative AI tools in 2022, courts may rethink the traditional application of Section 230. As the statute states, "The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[105] Generative AI platforms, such as the ones used to create deepfake pornography, blur the line between an online service provider and an "information content provider" because the platform itself is generating the content.[106] In fact, Justice Neil Gorsuch has questioned the applicability of Section 230 for generative AI platforms: "Artificial intelligence generates poetry. It generates polemics today that would be content that goes beyond picking, choosing, analyzing, or digesting content. And that is not protected. Let's assume that's right. Then the question becomes, what do we do about recommendations?"[107]

Although Section 230 may become inapplicable to generative AI platforms in the future, this Note will analyze the possible liability frameworks as they are currently understood and applied by courts.

B. Tort Law

Tort law may provide recourse for a subset of victims, but the applicability and outcomes for victims seeking redress under tort law are scattered and inconsistent. A prominent barrier for victims receiving legal redress under tort law is Section 230.[108] Since tort law comes from state civil laws, victims cannot sue AI or web platforms but instead must identify, find, and serve the individual

---

101. *See generally* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 404 (2017) ("Section 230 immunity has enabled innovation and expression beyond the imagination of the operators of early bulletin boards and computer service providers the provision was designed to protect. But its overbroad interpretation has left victims of online abuse with no leverage against site operators whose business models facilitate abuse.").

102. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1795 (2019).

103. *See id.*

104. *See id.* at 1792, 1795.

105. 47 U.S.C. § 230(f)(3).

106. Matt Perault, *Section 230 Won't Protect ChatGPT*, LAWFARE (Feb. 22, 2023), https://www.lawfaremedia.org/article/section-230-wont-protect-chatgpt [https://perma.cc/EM7S-3DT8].

107. *Id.*

108. *See supra* Section II.A.

perpetrators.[109] If the perpetrator distributes the deepfake anonymously, does not live in the United States, or does not have enough money to provide damages, victims may be left with no legal recourse.[110]

Moreover, victims often have the First Amendment working against them. The Supreme Court has set different standards for plaintiffs to recover for a content-based harm.[111] For public officials and public figures, they must prove "actual malice"—that is, knowledge of falsity or reckless disregard for the truth—with clear and convincing evidence in order to recover for a defamatory falsehood[112] or other content-based harm.[113] In contrast, private individuals must prove that the harmful material was published with at least negligence on behalf of the publisher, a lower standard than that of "actual malice."[114] This means that in addition to the statement being false, the perpetrator knew it was false or did not do enough to make sure it was true.[115] Specifically, three common law tort doctrines may provide recourse for victims: defamation, false light invasion of privacy, and intentional infliction of emotional distress.

1. Defamation

Defamation may provide a remedy for a subset of victims. Generally, a defamation claim requires proving the perpetrator (1) made a false and defamatory statement about the victim, (2) to a third party, (3) with fault of at least negligence on behalf of the perpetrator, and (4) the victim was harmed from the publication.[116] The nature of deepfake pornography would make the intent requirements—both negligence and actual malice—more manageable because, by definition, deepfakes are false depictions of people doing things they never did.[117] Perpetrators cannot claim ignorance of a deepfake's falsity after taking the time to create the fabricated media.[118] However, media that never purports to be authentic is not necessarily considered defamatory.[119] Thus, deepfakes that are obviously inauthentic or even just labeled as inauthentic may evade liability under a defamation claim.[120] Moreover, defamation requires that the false material be communicated to a third party.[121] This essentially bars claims where the deepfake is part of a harassment or blackmailing scheme solely between the perpetrator and victim.[122]

---

109. *See* 47 U.S.C. § 230.

110. *See* Chesney & Citron, *supra* note 102, at 1792.

111. *See generally* Hustler Mag., Inc. v. Falwell, 485 U.S. 46 (1988); Curtis Publ'g Co. v. Butts, 388 U.S. 130 (1967); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974).

112. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964).

113. *See Hustler Mag.*, 485 U.S. at 56; *see also Curtis Publ'g Co.*, 388 U.S. at 134.

114. *See Gertz*, 418 U.S. at 350.

115. Dallin Albright, *Do Androids Defame with Actual Malice? Libel in the World of Automated Journalism*, 75 FED. COMM. L.J. 103, 111 (2022).

116. RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

117. Pascale, *supra* note 60, at 346.

118. *Id.*

119. Milkovich v. Lorain J. Co., 497 U.S. 1, 20 (1990).

120. Pascale, *supra* note 60, at 347.

121. Wang, *supra* note 7, at 441.

122. *Id.*

2. False Light Invasion of Privacy

False light invasion of privacy may also provide a subset of victims with redress for harms caused by deepfake pornography. This doctrine generally provides that one who gives "publicity" to a matter that places another in a false light is liable if (1) the false light is highly offensive to a reasonable person, and (2) the actor knew of or acted in reckless disregard as to the falsity of the matter and the subsequent false light the victim was placed in.[123] The first element is likely met due to the offensive nature of deepfake pornography, and the second element is likely met because the creation of a deepfake requires the creation of something false.[124] However, the "publicity" requirement may pose an issue for plaintiffs.[125] "Publicity" under a false light claim means that the matter was communicated to the public at large or to a large enough audience that the matter is "substantially certain to become one of public knowledge."[126] For celebrities, public figures, and others who find deepfake pornography of them a newsworthy matter, this requirement may not pose an issue. For others, however, such as those who were victims of deepfake pornography shared to a limited group, posted on a niche website, or used as a harassment tool, it may not be possible to bring a valid claim under false light invasion of privacy.[127]

3. Intentional Infliction of Emotional Distress

Under the doctrine of intentional infliction of emotional distress ("IIED"), a small subgroup of victims may be able to recover for deepfakes made against them. Although state doctrines vary, most require victims to show that (1) the creator intended to (2) cause the victim severe emotional distress (3) by extreme and outrageous conduct, and (4) the victim did, in fact, suffer severe emotional distress as a result of such extreme and outrageous conduct.[128] Victims would likely prove the third element because deepfakes would likely constitute conduct "beyond the bounds of human decency, such that it would be regarded as intolerable in a civilized community."[129] Victims are also likely to succeed on the fourth element, where they can prove that their emotional distress is "so severe that no reasonable [woman] could be expected to endure it."[130] Where the majority of victims will fail on an IIED claim, however, is proving the intent of the creator.[131] Perpetrators of deepfake pornography are often looking to fulfill a sexual desire and do not intend for the victim to watch, or even know about, the deepfake's existence.[132] In instances where perpetrators send a deepfake to the victim or otherwise notify them to cause harm, IIED may be a path to recourse for victims.[133] However, for victims who stumble

123. RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1977).
124. Wang, *supra* note 7, at 442.
125. *Id.*
126. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (AM. L. INST. 1977).
127. Wang, *supra* note 7, at 442.
128. Douglas Harris, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99, 111 (2019).
129. *Id.*
130. *Id.* (quoting RESTATEMENT (SECOND) OF TORTS § 46 (AM. L. INST. 1965)).
131. *Id.* at 112.
132. *Id.*
133. *Id.*

upon a deepfake of themselves or are made aware by a third party of its existence, this common law remedy will not provide recourse.[134]

C. Intellectual Property Law

Intellectual property law may provide recourse for a subset of victims of deepfake pornography.[135] In select circumstances and jurisdictions, victims may seek relief through copyright law or statutes protecting the right of publicity. However, because of affirmative defenses and specific legal requirements, neither provides a perfect path to legal recourse for victims.[136]

1. Copyright

Victims may be able to claim that deepfake pornography infringes on the copyrights of the original media used to create the deepfake.[137] One benefit to this solution is that victims would be able to sidestep the bar presented by Section 230.[138] Since Section 230 does not provide immunity for violations of intellectual property laws, victims would be able to sue platforms and original perpetrators alike for copyright infringement.[139] This first requires, however, that victims own the copyright to the media in the first place.[140] Ownership of a copyrighted work belongs to the "creative mastermind" of the creation.[141] The victim may qualify as the creative mastermind if she took the photo or video herself.[142] However, if someone else took the photos or videos, the creative mastermind would not be the victim, and, therefore, she would not be entitled to any copyright of the material.[143]

Even if a victim does own the copyrights of the media used to create the deepfake, a copyright infringement claim may nonetheless fail under the affirmative defense of fair use.[144] Fair use is a safe haven for criticism, comment, news reporting, teaching, scholarship, and research to promote the public interest.[145] When evaluating whether a work constitutes fair use, courts consider four factors: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the amount and substantiality of the work, and (4) the effect of the use upon the potential market.[146] The first factor, purpose and character of the use, may weigh in favor of deepfake pornography being fair use.[147] This factor heavily considers how

---

134. *Id.*
135. *See* Gieseke, *supra* note 37, at 1501–02.
136. *See id.*
137. *Id.* at 1501.
138. *See* 47 U.S.C. § 230(e)(2); *see also* Lindsey Joost, *The Place for Illusions: Deepfake Technology and the Challenges of Regulating Unreality*, 33 U. FLA. J.L. & PUB. POL'Y 309, 329 (2023) ("[T]he scope of [Section 230] does not cover intellectual property breaches, so if a party holds copyright to the image, the takedown request must be executed pursuant to the Digital Millennium Copyright Act.").
139. 47 U.S.C. § 230; *see supra* Section II.A.
140. Gieseke, *supra* note 37, at 1500.
141. 17 U.S.C § 201.
142. *Id.*
143. Gieseke, *supra* note 37, at 1501.
144. 17 U.S.C § 107.
145. *Id.*
146. *Id.*
147. Gieseke, *supra* note 37, at 1500–01.

"transformative" the infringing work is, or how much it transforms the original work into something new.[148] Since fair use can be asserted as an affirmative defense, deepfake pornography that constitutes fair use would effectively bar any copyright claims a victim could bring.[149]

2. Right of Publicity

Victims of deepfake pornography may be able to claim that the material infringed on their right of publicity. The right of publicity is an intellectual property right that "protects against the misappropriation of a person's name, likeness, or other indicia of personal identity—such as nickname, pseudonym, voice, signature, likeness, or photograph—for commercial benefit."[150] While this approach may provide a remedy against a large corporation using an individual's name, image, or likeness for commercial purposes, it does not provide much recourse for victims of deepfake pornography who are victimized by "passion projects" of the creators.[151] If the deepfake media is not used for commercial benefit, the right of publicity may not apply at all and thus may not provide any recourse.[152]

If the deepfake media was found to be used for commercial purposes (such as generating advertisement revenue, for example) a right of publicity claim would depend on applicable state laws.[153] Currently, no federal law governs the right of publicity,[154] and 20 states do not recognize the right at all.[155] Among the states that recognize the right of publicity, the types of people and aspects protected and the post-mortem protections, defenses, and exceptions vary widely.[156] Moreover, the potential defendants to a right of publicity claim also depend on the jurisdiction. Circuits are split on whether the intellectual property exception under Section 230 applies to state intellectual property rights, such as the right of publicity, or whether they apply solely to federally recognized intellectual property rights, such as trademarks, copyrights, and patents.[157] Thus, whether a victim can sue the platforms for infringing on her right of publicity depends on the jurisdiction.

---

148. The infringing work can be considered transformative if it creatively transforms the work or transforms its purpose or character. Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

149. de Guzman, *supra* note 29, at 119.

150. *Right of Publicity*, INT'L TRADEMARK ASS'N, https://www.inta.org/topics/right-of-publicity/ [https://perma.cc/5BSG-VERG] (last visited Nov. 27, 2023); *see also* Benjamin T. Suslavich, *Nonconsensual Deepfakes: A "Deep Problem" For Victims*, 33 ALB. L.J. SCI. & TECH. 160, 175 (2021).

151. Suslavich, *supra* note 150, at 175.

152. *Id.*

153. *Id.* at 177.

154. *Right of Publicity*, *supra* note 150.

155. Right of Publicity Committee, *Right of Publicity State of the Law Survey*, INT'L TRADEMARK ASS'N, https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/INTA_2019_rop_survey.pdf [https://perma.cc/V2VM-NLAE] (last visited Nov. 27, 2023).

156. *Id.*

157. BRANNON & HOLMES, *supra* note 71, at 28–29; *see supra* Section II.A.

D. Federal Law

On a federal level, several laws dance around deepfakes but do not directly address the harms they cause to victims. For example, the National Defense Authorization Act for Fiscal Year 2020 requires that the Director of National Intelligence submit a report to congressional intelligence committees detailing potential national security threats due to deepfakes.[158] Similarly, in October 2023, the Biden Administration released a broad Executive Order ("Order") that permits the federal government to enforce requirements on AI models before the model can be used.[159] The Order prioritizes consumer welfare while maintaining the United States' position as a leader in AI.[160] Although this "sweeping action" is the federal government's first major effort in enacting safety assessments, equity and civil rights guidance, and research on AI's impact, it does little to deter nonconsensual deepfake pornography.[161] Rather, the Order requires the Department of Commerce to develop guidance for content authentication, such as watermarking, to clearly label AI-generated content.[162] While this will protect Americans from AI-enabled fraud, it does not provide legal recourse for victims depicted in AI-generated pornography.

Thus far, no federal legislation regulating deepfakes has been passed, although some lawmakers have tried.[163] Some of these proposed laws target deepfakes generally, not just deepfake pornography. For example, Senator Ben Sasse proposed the Malicious Deep Fake Prohibition Act in 2018, which would have criminalized creating or knowingly distributing a deepfake with the intent to "facilitate criminal or tortious conduct under Federal, State, local, or Tribal law."[164] This Act did not prohibit specific uses of deepfakes; rather, it created additional grounds for liability for facilitating illegal or tortious conduct.[165] The bill did not make it out of committee.[166]

Similarly, in 2019, Representative Yvette Clarke introduced the Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act ("DEEPFAKES Accountability Act").[167] This Act would have

---

158. 50 U.S.C. § 3369a.

159. *See* Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023); Charley F. Brown & Jonathan P. Hummel, *Executive Order Allows Federal Government to Regulate AI Models*, BALLARD SPAHR (Oct. 30, 2023), https://www.ballardspahr.com/Insights/Alerts-and-Articles/2023/10/Executive-Order-Allows-Federal-Government-to-Regulate-AI-Models [https://perma.cc/R2H3-8L4C].

160. *See* Exec. Order No. 14,110, 88 Fed. Reg. at 75191.

161. *See* Brown & Hummel, *supra* note 159.

162. *Id.*

163. Pascale, *supra* note 60, at 342–43; *see, e.g.*, Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019, H.R. 3230, 116th Cong. (2019) (introduced by Rep. Yvette Clarke); Malicious Deep Fake Prohibition Act of 2018, S. 3805, 115th Cong. (2018) (introduced by Senator Ben Sasse).

164. S. 3805; Jack Langa, *Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfakes*, 101 B.U. L. REV. 761, 778 (2021).

165. Langa, *supra* note 164, at 778–79.

166. Wang, *supra* note 7, at 426.

167. H.R. 3230.

required that any "advanced technological false personation record with the intent to distribute such record over the internet" be labeled with a watermark or other identifying trait indicating that it is a deepfake.[168] Further, a person who knowingly fails to disclose that content is a deepfake would face criminal and civil liability, including up to five years imprisonment and a fine.[169] This Act also provides for an exception for deepfake media where "a reasonable person would not mistake the falsified material activity for actual material activity of the exhibited living person."[170] The bill has not progressed since being referred to a subcommittee.[171]

However, lawmakers have recently introduced legislation that specifically targets deepfake pornography. For example, the Preventing Deepfakes of Intimate Images Act, introduced in May 2023 by Representative Joseph Morelle, provides victims of deepfake pornography a private right of action for disclosures of "intimate digital depictions" without the depicted individual's voluntary and informed consent in writing.[172] Under the Act, victims can recover disgorgement of the perpetrator's profits, up to $150,000 in statutory damages, punitive damages, and attorney's fees, as well as injunctive relief.[173] The Act also criminalizes the nonconsensual disclosure or threat of disclosure of deepfake pornography "(1) with the intent to harass, annoy, threaten, alarm, or cause substantial harm to the . . . depicted individual; or (2) with actual knowledge that, or reckless disregard for whether, such disclosure or threatened disclosure will cause physical, emotional, reputational, or economic harm to the depicted individual."[174] Criminal remedies under the Act include fines, imprisonment up to ten years, or both.[175] Interestingly, under both the civil and criminal prongs of the Act, it is not a defense to include a disclaimer stating that the media is nonconsensual or that the media is a deepfake.[176] The Act also mirrors the immunity for online service providers under Section 230 in both the civil and criminal contexts.[177] This is especially worrisome in the criminal context because Section 230 specifically sets out an exception for federal criminal law.[178] By providing more immunity than Section 230 already provides service providers, this Act creates an even bigger barrier for victims to find relief. This Act has not progressed since being referred to subcommittee.[179]

The Disrupt Explicit Forged Images And Non-Consensual Edits Act of 2024 ("DEFIANCE Act"), introduced by Senator Dick Durbin in January 2024, also provides a civil right of action for victims of nonconsensual deepfake

168. *Id.*; Langa, *supra* note 164, at 779; Wang, *supra* note 7, at 426.
169. H.R. 3230; Langa, *supra* note 164, at 779.
170. H.R. 3230; Langa, *supra* note 164, at 779.
171. Wang, *supra* note 7, at 426.
172. Preventing Deepfakes of Intimate Images Act, H.R. 3106, 118th Cong. § 2 (2023).
173. *Id.*
174. *Id.* § 3.
175. *Id.*
176. *Id.* §§ 2–3.
177. *Id.*
178. 47 U.S.C. § 230(e)(1).
179. *H.R.3106 - Preventing Deepfakes of Intimate Images Act*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/3106/all-actions?s=1&r=64 [https://perma.cc/5KHA-NKP4] (last visited Mar. 22, 2024).

pornography.[180] This Act not only provides a right of action for the nonconsensual disclosure of deepfake pornography but also provides a right of action for the nonconsensual *production* of deepfake pornography.[181] Victims are able to recover actual damages, liquidated damages up to $150,000, attorney's fees, and injunctive relief.[182] This Act has not progressed since being referred to subcommittee.[183]

Most recently, another piece of legislation, the Protect Victims of Digital Exploitation and Manipulation Act of 2024, specifically criminalizes deepfake pornography.[184] Introduced in March 2024 by Representative Nancy Mace, this Act makes it a crime to "knowingly or recklessly" produce or distribute a "digital forgery of an identifiable individual" without the individual's voluntary and informed consent.[185] Perpetrators can face statutory fines, up to five years in prison, or both.[186] This Act exempts online service providers from criminal liability, therefore extending the immunity provided to online service providers under Section 230.[187] By providing more immunity than Section 230 already provides service providers, this Act continues to perpetuate a barrier to victims finding relief. This Act has not progressed since being referred to subcommittee.[188]

E. State Law

Although most states have passed laws on nonconsensual pornography,[189] few have expanded these laws to deepfake pornography.[190] As of September 2024, the federal government, 49 states, the District of Columbia, the territory of Guam, and the Uniform Code of Military Justice have laws on nonconsensual pornography.[191] In contrast, only 11 states have passed laws that specifically

---

180. DEFIANCE Act of 2024, S. 3696, 118th Cong. § 3 (2024).

181. *Id.*

182. *Id.*

183. *S.3696 - DEFIANCE Act of 2024*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/senate-bill/3696/text [https://perma.cc/4X7K-6DAJ] (last visited Mar. 22, 2024).

184. Protect Victims of Digital Exploitation and Manipulation Act of 2024, H.R. 7567, 118th Cong. § 2 (2024).

185. *Id.*

186. *Id.*

187. *Id.*

188. *H.R.7567 - Protect Victims of Digital Exploitation and Manipulation Act of 2024*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/7567/text [https://perma.cc/53ZW-TXJX] (last visited Mar. 22, 2024).

189. FRANKS, *supra* note 45, at 5 ("As of October 2021, forty-eight state legislatures, the District of Columbia, the territory of Guam, and the Uniform Code of Military Justice have recognized the devastating impact of this form of privacy violation through criminal statutes.").

190. Pascale, *supra* note 60, at 344.

191. *See* 15 U.S.C. § 6851; *see also Nonconsensual Pornography (Revenge Porn) Laws in the United States*, BALLOTPEDIA, https://ballotpedia.org/Nonconsensual_pornography_(revenge_porn)_laws_in_the_United_States [https://perma.cc/YP63-UFYA] (last visited Mar. 18, 2024); FRANKS, *supra* note 45, at 5. In addition, Massachusetts passed a bill criminalizing nonconsensual sharing of explicit images, which took effect on September 18, 2024. MASS. GEN. LAWS ch. 265, § 43A(b)(2) (2024); *Press Release: Governor Healey*

encompass nonconsensual *deepfake* pornography.[192] The laws vary widely among these states, making victims' protections and rights change depending on their location. Nonetheless, Section 230 continues to present a barrier for victims regardless of where in the country they reside. Section 230(e)(3) does not provide immunity for online service providers when they violate state laws that are "consistent" with Section 230.[193] Where state civil or criminal laws are inconsistent with Section 230, Section 230 preempts the state law and provides immunity to service providers.[194] Thus, Section 230 still presents an indirect, but prominent, barrier for victims bringing claims under state deepfake pornography law: they must identify and sue the original individual distributor.

1. Civil Remedies

Two states, California and Illinois, provide exclusively civil remedies for victims of deepfake pornography.[195] Florida, New York, and Minnesota provide victims with a private right of action in addition to criminalizing the dissemination of deepfake pornography.[196]

Both California and Illinois adapted their nonconsensual pornography laws to encompass deepfake pornography. Under California's law, victims have a private right of action against any person who (1) "[c]reates and intentionally discloses sexually explicit material if that person knows or reasonably should have known the depicted individual did not consent," or (2) "[i]ntentionally discloses sexually explicit material that the person did not create if the person knows the depicted individual did not consent."[197] Under the statute, the term "depicted individual" includes individuals "who [appear], as a result of digitization, to be giving a

---

Signs Bill Banning Revenge Porn, Expanding Protections Against Abuse and Exploitation, COMMONWEALTH OF MASS. (June 20, 2024), https://www.mass.gov/news/governor-healey-signs-bill-banning-revenge-porn-expanding-protections-against-abuse-and-exploitation [https://perma.cc/H5L6-8WS8].

192. *"Deep Fake" or Synthetic Media Laws*, CYBER C.R. INITIATIVE (Sept. 22, 2021), https://cybercivilrights.org/deep-fake-laws/ [https://perma.cc/FW87-GGX4]; MASS. GEN. LAWS ch. 265, § 43A(b)(2) (2024). Note that several more states have laws specifically banning deepfakes depicting minors, but because of the nuances surrounding child pornography generally, this Note focuses only on laws that prohibit deepfake pornography among adults. For the overlap between deepfake pornography and "morphed" child pornography, see Pascale, *supra* note 60.

193. 47 U.S.C. § 230(e)(3).

194. Voicenet Commc'ns, Inc. v. Corbett, No. 04-1318, 2006 WL 2506318, at *3 (E.D. Pa. Aug. 30, 2006) ("When subsection (e) is examined as a whole, it becomes even more clear that sub-subsection (e)(3) gives interactive computer service providers immunity from state criminal laws that are inconsistent with the CDA."); BRANNON & HOLMES, *supra* note 71, at 27; *see supra* Section II.A.

195. *See* CAL. CIV. CODE § 1708.86(a)(4) (2020); 740 ILL. COMP. STAT. 190/10 (2024).

196. FLA. STAT. § 836.13(4)–(5) (2022); N.Y. CIV. RIGHTS LAW § 52-b (McKinney 2024); MINN. STAT. § 604.32 (2023).

197. K.C. Halm, et al., *Two New California Laws Tackle Deepfake Videos in Politics and Porn*, DAVIS WRIGHT TREMAINE LLP (Oct. 11, 2019), https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2019/10/california-deepfakes-law [https://perma.cc/4FX3-27CP]; CAL. CIV. CODE § 1708.85(a) (2022).

performance they did not actually perform or to be performing in an altered depiction."[198]

Under Illinois's law, someone who is "identifiable to a reasonable person" has a private right of action against another who disseminated a "private or intentionally digitally altered sexual image without the depicted individual's consent."[199] Additionally, the perpetrator must have "kn[own] or recklessly disregarded the possibility" that: (1) the depicted individual did not consent to the dissemination; (2) the image was a private or intentionally digitally altered sexual image; and (3) the depicted individual was identifiable.[200] Both states provide exceptions for matters of public concern, reporting purposes, law enforcement purposes, and legal proceedings.[201] Notably, disclosing that the material is digitally altered or that the depicted individual did not participate in its creation is not a defense to liability under both laws.[202]

While providing a private right of action offers victims at least some form of redress, it is not the best option for victims of deepfake pornography. To be sure, civil litigation does provide benefits to plaintiffs, such as a lower burden of proof, more control throughout the case, recovery of monetary damages, and increased privacy measures during litigation.[203] Nonetheless, the nature of deepfake pornography makes recovery difficult in civil cases. Due to Section 230, even finding a defendant to sue can be a major hurdle preventing a civil lawsuit because of the anonymity provided by the internet.[204] Even where the victim can find a defendant to sue, the defendant may be unable to pay monetary damages, resulting in a "judgment proof" defendant.[205] Civil remedies, despite being a step in the right direction, are not the best remedy for victims of deepfake pornography.

2. Criminal Remedies

The other nine states with laws on deepfake pornography (Hawaii,[206] Florida,[207] Georgia,[208] Massachusetts,[209] Minnesota,[210] New York,[211] South Dakota,[212] Texas,[213] and Virginia[214]) criminalize the dissemination of the explicit

198. CAL. CIV. CODE § 1708.86(a)(4) (2020).
199. 740 ILL. COMP. STAT. 190/10(a) (2024).
200. *Id.*
201. CAL. CIV. CODE § 1708.86(c) (2020); 740 ILL. COMP. STAT. 190/15(a) (2024).
202. 740 ILL. COMP. STAT. 190/10(c) (2024); CAL. CIV. CODE § 1708.86(d) (2020); *see also* Van Lier, *supra* note 44, at 20.
203. *Civil Remedies*, THE ADVOCS. FOR HUM. RTS. (Feb. 10, 2009), https://www.stopvaw.org/civil_remedies [https://perma.cc/YKU4-ENY9].
204. *See* Chesney & Citron, *supra* note 102, at 1792; *see supra* Section II.A.
205. Chesney & Citron, *supra* note 102, at 1792–93.
206. HAW. REV. STAT. § 711-1110.9 (2021).
207. FLA. STAT. § 836.13 (2022).
208. GA. CODE § 16-11-90 (2022).
209. MASS. GEN. LAWS ch. 265, § 43A(b)(2) (2024).
210. MINN. STAT. § 617.262 (2023).
211. N.Y. PENAL LAW § 245.15 (McKinney 2023).
212. S.D. CODIFIED LAWS § 22-21-4(3) (2023).
213. TEX. PENAL CODE § 21.165 (2023).
214. VA. CODE § 18.2-386.2 (2024).

material. Among these states' laws are similarities and differences that alter the protections for victims in each state.

Generally, every state outlaws the dissemination of deepfake pornography without the consent of the person depicted.[215] Texas is unique in that it also prohibits *producing* deepfake pornography under its law.[216] States also unanimously provide an exception for the service providers hosting the deepfake content, mirroring Section 230's immunity provided to online service providers.[217] Georgia is unique in that it only provides a rebuttable presumption that online service providers do "not know the content of an electronic transmission or post"; therefore, it does not give service providers complete blanket immunity.[218] Several states also include public policy exceptions in their laws, such as for law enforcement, legal proceedings, and medical treatment.[219] Furthermore, states almost uniformly require malicious intent on behalf of the perpetrator to violate the law.[220] Virginia, for example, requires that the deepfake is "maliciously" disseminated with "the intent to coerce, harass, or intimidate."[221] Minnesota is unique in that its law only requires perpetrators to "intentionally" disseminate the deepfake.[222] When determining penalties, however, the law provides harsher penalties for deepfakes that were disseminated with the intent to profit from the material or to harass the depicted individual.[223]

States differ in the nuances of each law, which can make a big difference for victims seeking recourse. First, states differ on the application of the laws and whether jurisdiction is dependent on where the victim lives, where the perpetrator lives, or both. Georgia makes it clear that a perpetrator is subject to prosecution in Georgia if they live outside of Georgia but the victim lives in Georgia, or if they live

---

215. *See, e.g.*, HAW. REV. STAT. § 711-1110.9 (2021); FLA. STAT. § 836.13 (2022); GA. CODE § 16-11-90 (2022); MINN. STAT. § 617.262 (2023); N.Y. PENAL LAW § 245.15 (McKinney 2023); S.D. CODIFIED LAWS § 22-21-4(3) (2022); VA. CODE § 18.2-386.2 (2024); MASS. GEN. LAWS ch. 265, § 43A(b)(2) (2024).

216. TEX. PENAL CODE § 21.165(b) (2023). For a discussion on why it is the dissemination, and not the creation, of deepfake pornography that should be criminalized, see Harris, *supra* note 128, at 125–28.

217. *See, e.g.*, HAW. REV. STAT. § 711-1110.9 (2021); FLA. STAT. § 836.13 (2022); GA. CODE § 16-11-90 (2022); MINN. STAT. § 617.262 (2023); N.Y. PENAL LAW § 245.15 (McKinney 2023); S.D. CODIFIED LAWS § 22-21-4(3) (2022); VA. CODE § 18.2-386.2 (2024); TEX. PENAL CODE § 21.165 (2023); MASS. GEN. LAWS ch. 265, § 43A(b)(2) (2024).

218. GA. CODE § 16-11-90(f) (2022).

219. *See, e.g.*, HAW. REV. STAT. § 711-1110.9 (2021); FLA. STAT. § 836.13 (2022); GA. CODE § 16-11-90 (2022); N.Y. PENAL LAW § 245.15 (McKinney 2023); TEX. PENAL CODE § 21.165 (2023).

220. *See, e.g.*, HAW. REV. STAT. § 711-1110.9 (2021); FLA. STAT. § 836.13 (2022); GA. CODE § 16-11-90 (2022); N.Y. PENAL LAW § 245.15 (McKinney 2023); S.D. CODIFIED LAWS § 22-21-4(3) (2022); VA. CODE § 18.2-386.2 (2024); TEX. PENAL CODE § 21.165 (2023).

221. VA. CODE § 18.2-386.2(A) (2024).

222. MINN. STAT. § 617.262(2) (2023).

223. *Id.*

within Georgia, regardless of the victim's residence.[224] On the other hand, some state statutes are silent on who is subject to prosecution under the state law.[225]

States also differ in their definitions of what qualifies as explicit deepfake material. While all states generally prohibit deepfakes depicting another person in the nude or in a sexual act, some states strictly define nudity as exposure of the genitals, pubic area, buttocks, or female breasts.[226] Other states take a broader view of the definition of nudity, thus expanding the scope of deepfakes prosecutable under the law.[227] Hawaii, for example, defines "nude" to mean "unclothed or in attire, including but not limited to sheer or see-through attire, so as to expose to view any portion of the pubic hair, anus, cleft of the buttocks, genitals or any portion of the female breast below the top of the areola."[228]

Another difference among states is the requirement that the deepfake causes a reasonable person to believe it was real.[229] South Dakota, for example, requires that the deepfake "would cause a reasonable person to mistakenly believe that the image or recording is authentic."[230] This caveat creates a large loophole for perpetrators who either label the explicit media as a deepfake or who disseminate lower-quality media that cannot be considered authentic but is harmful nonetheless.[231] A better approach is evident in Florida's law—it provides that a disclaimer "which notifies a viewer that the person or persons depicted did not consent to or participate in the creation . . . is not a defense and does not relieve a person of criminal liability."[232] This closes the loophole for perpetrators who simply label the media as a deepfake.

F. Applying Principles of Nonconsensual Pornography Laws to Deepfake Pornography

Although few jurisdictions have adapted their nonconsensual pornography statutes to cover deepfake pornography, nonconsensual pornography laws can still provide meaningful guidance when crafting legislation for deepfake pornography. Dr. Mary Anne Franks, through the Cyber Civil Rights Initiative ("CCRI"), created a guide for legislators on the best practices to adhere to when creating laws on nonconsensual pornography.[233] Although not all laws reflect the recommendations of Franks and the CCRI, the CCRI has advised the majority of states on drafting

---

224. GA. CODE § 16-11-90(d) (2022).

225. *See, e.g.*, HAW. REV. STAT. § 712-1210 (2021); N.Y. PENAL LAW § 245.15 (McKinney 2023); S.D. CODIFIED LAWS § 22-21-4 (2022); TEX. PENAL CODE § 21.165 (2023); VA. CODE ANN. § 18.2-386.2 (2024).

226. *See, e.g.*, S.D. CODIFIED LAWS § 22-21-4 (2022); TEX. PENAL CODE § 21.165 (2023); N.Y. PENAL LAW § 245.15 (McKinney 2023); MINN. STAT. § 617.262 (2023).

227. *See, e.g.*, HAW. REV. STAT. § 712-1210 (2021); FLA. STAT. § 836.13 (2022); GA. CODE § 16-11-90 (2022).

228. HAW. REV. STAT. § 712-1210 (2021).

229. *See, e.g.*, TEX. PENAL CODE § 21.165 (2023); MINN. STAT. § 617.262 (2023); S.D. CODIFIED LAWS § 22-21-4 (2022).

230. S.D. CODIFIED LAWS § 22-21-4(3)(a) (2022).

231. *See* Pascale, *supra* note 60, at 345.

232. FLA. STAT. § 836.13(4) (2022).

233. *See generally* FRANKS, *supra* note 45.

their nonconsensual pornography statutes.[234] The following discussion highlights heuristics in the CCRI's guide that should also apply to deepfake pornography statutes.

The CCRI recommends that nonconsensual pornography laws should clearly set out the elements of the offense, with the three basic elements being: (1) the disclosure of private, sexually explicit photos or videos; (2) of an identifiable person; (3) without the consent of the person depicted.[235] The recommended mens rea for the first element should be purpose or knowledge to avoid punishment for purely accidental disclosures.[236] The CCRI also recommends that the mens rea for the third element should be no higher than recklessness: "[F]or an offender to be punished, he would have to have known that there was a substantial risk that the person depicted had not consented to the disclosure and be unable to offer justification for why he took that risk."[237]

These suggestions for mens rea requirements can apply to laws on deepfake pornography as well. It is true that the creation of deepfake pornography will rarely, if ever, be accidental. But it is mainly the disclosure of deepfake pornography that any legislation should criminalize.[238] This is because although the creation of deepfake pornography can be an invasion of privacy, the true harm occurs when the media is disclosed to others in a way that is embarrassing and jeopardizing to victims.[239] Therefore, any legislation should prevent punishment for purely accidental disclosures.[240] Moreover, consensual deepfakes should not be criminalized and can actually be a positive form of sexual expression when used in a private and consensual manner.[241] Legislation should, therefore, only focus on the disclosure of nonconsensual pornographic deepfakes.

For nonconsensual pornography statutes, the CCRI suggests that they should not require that perpetrators act with the intent to harass, humiliate, or cause emotional distress.[242] Such a requirement not only misclassifies nonconsensual pornography as a form of harassment instead of an invasion of privacy, but it also potentially renders statutes vulnerable to First Amendment challenge.[243] While motive requirements like these are not required in criminal laws or in laws regulating

---

234. *Id.* at 5.
235. *Id.* at 7–8.
236. *Id.* at 8.
237. *Id.*
238. Harris, *supra* note 128, at 125–28.
239. *Id.* at 125.
240. *Id.* at 126. The criminalization of possession of deepfake pornography may also open any legislation to First Amendment challenge. *Id.* at 127–28 (explaining that "[a] statute banning all deepfakes depicting pornography will likely be unconstitutionally overbroad" because, among other considerations, "individuals do not have a right to prevent others from tampering with images in the privacy of their own homes and for personal use").
241. Chesney & Citron, *supra* note 102, at 1771 ("[I]ndividuals suffering from certain physical disabilities might interpose their faces and that of consenting partners into pornographic videos, enabling virtual engagement with an aspect of life unavailable to them in a conventional sense.").
242. FRANKS, *supra* note 45, at 9.
243. *Id.*

expression, they open the door to First Amendment challenge because the Supreme Court considers terms like "harass," "torment," and "embarrass" as unconstitutionally vague.[244]

In terms of legislation on deepfake pornography, laws should also avoid naming specific intents for the same reasons. Perpetrators of deepfake pornography create the harmful media for a plethora of reasons, yet all cause immense harm to victims when distributed.[245] To avoid another imperfect legal remedy that is available to some subclasses of victims but not others, legislation on deepfake pornography should avoid naming specific intent requirements.

The CCRI emphasizes providing an appropriate scope for nonconsensual pornography statutes. The law should not be so broad as to include drawings or other overbroad definitions of nudity in its scope,[246] but it should not be so narrowly drafted that it *only* applies to images featuring nudity or images made through high-tech means.[247] On the one hand, having a law that is too broad can lead to the criminalization of artistic pursuits, such as drawings, or the "baby in the bath" problem, where parents would face criminal liability for posting innocent pictures of their naked infants.[248] On the other hand, having a law that is too narrow would not recognize the different types of harmful nonconsensual pornography; an image can be sexually explicit without containing nudity,[249] and it can still be harmful if disclosed through low-tech means, such as printed photographs and DVDs.[250]

When it comes to legislation on deepfake pornography, it is important to include an appropriate scope as well, but for different reasons. Arguably, it is important to have a somewhat broader scope for deepfake pornography laws. Unlike nonconsensual pornography, there is not a risk of the "baby in the bath" problem with deepfake pornography because the act of creation inherently removes any innocuous claims.[251] Although deepfake pornography is not always completely fabricated like a drawing, it can be with generative AI that creates the explicit images itself.[252] AI as a medium of creation is also much more harmful than a drawing because of how realistic the media can be and the scale at which the media can be

---

244. *Id.* at 11.

245. Hailey Reissman, *What Is Deepfake Porn and Why Is It Thriving in the Age of AI?*, ANNENBERG SCH. FOR COMMC'N (July 13, 2023), https://www.asc.upenn.edu/news-events/news/what-deepfake-porn-and-why-it-thriving-age-ai [https://perma.cc/ZWH2-7MAW] ("Creating fake erotic images is not inherently bad; online spaces can be a great way to explore and enjoy your sexuality. However, when fake nude images of people are created and distributed without their consent, it becomes deeply harmful.").

246. FRANKS, *supra* note 45, at 11.

247. *Id.* at 12.

248. *Id.* at 11.

249. *Id.* at 12.

250. *Id.*

251. For the overlap between deepfake pornography and "morphed" child pornography, see Pascale, *supra* note 60, at 350–65.

252. *See* HENRY ADJER ET AL., THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT 8 (2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf [https://perma.cc/AB75-NUF7].

created.[253] Moreover, expansive definitions of nudity may be able to adequately cover the varying levels of harm that deepfake pornography can cause victims. Although a deepfake with covered yet visible genitals is arguably not as harmful as that of "hardcore" pornography, it still can cause major embarrassment and reputational harm to the victim. Similarly, although deepfakes made with older technologies like Photoshop may be less realistic than those made with artificial intelligence, they can still be harmful to victims.

For nonconsensual pornography statutes, the CCRI also sets out narrow exceptions, such as for sexually explicit images voluntarily exposed in public or commercial settings,[254] and exceptions for disclosures made in the public interest, such as the lawful practices of law enforcement or medical treatment.[255] These exceptions are intended to prevent prosecution for individuals reporting public flashing or linking to websites for what they reasonably believe is commercial pornography, as well as for legitimate law enforcement and medical purposes.[256]

In terms of deepfake pornography, similar exceptions should apply to any legislation. First, the law should avoid prosecuting individuals who distribute deepfake pornography in a commercial context, given that they reasonably believe the material to be commercial pornography and not a deepfake. Second, the law should avoid prosecuting individuals for reporting known deepfakes to the appropriate resource, such as online service providers, law enforcement, or other advocacy groups or organizations. It is especially important for law enforcement to have access to deepfake pornography to support criminal investigations.[257] Further, although medical treatment is not necessary because the depicted sexual acts did not actually happen, an exception can be made for reporting instances of deepfake pornography to advocacy groups or other organizations to receive help.[258]

The CCRI also suggests that a nonconsensual pornography law should not be limited to conduct perpetrated by a current or former intimate partner.[259] It is important that this same heuristic apply to legislation on deepfake pornography because often, in the cases of celebrities victimized by deepfake pornography, for example, the harmful act is perpetrated by complete strangers.[260] Since deepfake pornography can be created by simply obtaining a picture of someone's face, legislation should not be confined to former or current intimate partners.[261]

Lastly, the CCRI suggests that a nonconsensual pornography law should not broaden immunities for online providers beyond what is already provided under Section 230.[262] As mentioned above, Section 230 provides immense protections for

253. *See id.*
254. FRANKS, *supra* note 45, at 9.
255. *Id.*
256. *Id.*
257. *See* MINN. STAT. § 617.262 (2023).
258. *See id.*
259. FRANKS, *supra* note 45, at 12.
260. *See* Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887, 896 (2019).
261. de Guzman, *supra* note 29, at 116.
262. FRANKS, *supra* note 45, at 12.

platforms hosting deepfake pornography, as well as major barriers for victims seeking a defendant to hold liable.[263] Thus, legislation on deepfake pornography also should not expand immunities beyond those provided under Section 230.

III. FUTURE LEGAL REMEDIES

A. The Case for Federal Criminal Law

An ideal law on deepfake pornography would be a federal statute that criminalizes the creation and dissemination of nonconsensual deepfake pornography while also providing a civil right of action. Congress is in the best position to legislate for three main reasons. First, states are unequipped to handle the issue adequately.[264] While state laws can provide decent solutions for their residents, adoption of deepfake pornography laws has been slow and inconsistent among states.[265] With technology becoming more widespread, sophisticated, and accessible, the stakes are too high to wait for states to regulate.[266] Regulation should be nationally consistent to ensure that "the punishment imposed and remedies provided [do] not depend on the state in which the victims or perpetrators reside."[267] Providing an array of patchworked protections will not adequately address victims' harms nationwide. Rather, it will only provide another incomplete legal remedy.

Second, Congress is in the best position to legislate because deepfake pornography does not conform to jurisdictional boundaries.[268] Perpetrators of deepfake porn may reside in one state while their victims reside in another or even several other states.[269] Many state statutes are unclear on whether the law applies if the victim resides in the state, if the perpetrator resides in the state, or both.[270] Deepfake pornography causes interstate and even international harm and is not a "local crime" that can be confined to a single state or jurisdiction.[271]

The third and arguably most important reason to provide a federal criminal law is to close the loophole Section 230 provides to internet service providers.[272] Recall that Section 230 protects platforms from liability for users' speech with few exceptions, one of which is in the case that platforms violate federal criminal law.[273] It is no surprise that the most effective and efficient way to stop the harms caused by deepfake pornography is to target the platforms that host and help distribute it. Unlike the whack-a-mole game that may come with prosecuting individual perpetrators, federal criminal law on deepfake pornography will finally give online

---

263. Chesney & Citron, *supra* note 102, at 1795.
264. Delfino, *supra* note 260, at 927.
265. *Id.*
266. *Id.*
267. *Id.*
268. *Id.*
269. *Id.*
270. *See supra* Section II.E.
271. Delfino, *supra* note 260, at 927.
272. *Id.*
273. 47 U.S.C. § 230(e)(1); *see also Section 230*, *supra* note 73.

service providers a deterrent to stop hosting and distributing deepfake pornography: criminal liability.[274]

B. Suggestion

Federal legislation on deepfake pornography should learn from current laws on deepfake pornography and nonconsensual pornography. To be sure, most statutes on nonconsensual pornography do not encompass deepfake pornography, and most state statutes on deepfake pornography do not provide the best remedy for victims. Nonetheless, Congress can take bits and pieces from state laws and nonconsensual pornography laws to craft an informed and effective federal criminal law on deepfake pornography. A successful law will consist of eight components: (1) clearly defined elements of the crime, (2) a broad definition of nudity, (3) a broad definition of "deepfake," (4) no specific intent requirements, (5) no disclaimer loophole, (6) exceptions for public policy, (7) no expansion of Section 230 protections, and (8) a civil right of action. Each of these elements is explained below.

1. Clearly Defined Elements of the Crime

A federal law on deepfake pornography should clearly set out the elements of the offense. Specifically, the law should criminalize the intentional disclosure of deepfake pornography that depicts an identifiable person in the nude or engaging in sexual conduct where the identifiable person did not consent to the disclosure of the explicit material. Under this definition, the elements would be (1) the intentional disclosure of the deepfake, (2) of an identifiable person in the nude or engaging in sexual conduct, and (3) the identifiable person did not consent to the disclosure.

2. Definition of Nudity

Congress should take a broad approach to defining nudity because deepfake pornography can still be sexually explicit without depicting an individual in the nude. The definition of "nude" should therefore mirror Hawaii's statute on deepfake pornography, which defines nude as "unclothed or in attire, including but not limited to sheer or see-through attire, so as to expose to view any portion of the pubic hair, anus, cleft of the buttocks, genitals or any portion of the female breast below the top of the areola."[275] Compared to other states' definitions, this is a broader definition of nudity that will ensure explicit deepfakes are still covered under federal law, even if they are not depicting complete nudity.

3. Definition of Deepfake

Federal legislation should also broadly explain what constitutes a deepfake. It should not be so specific that only deepfakes created with AI are covered. Instead, the law should cover all "technologically made" explicit material. Virginia's deepfake pornography statute, for example, prohibits "any videographic or still image created by any means whatsoever."[276] Keeping the door open for all technologically made deepfakes will not only cover deepfakes made with

---

274. *See* Delfino, *supra* note 260, at 928; *see also supra* Section II.A. Enacting a federal criminal law may also add a level of severity and urgency that victims deserve. Delfino, *supra* note 260, at 928.

275. HAW. REV. STAT. § 712-1210 (2021).

276. VA. CODE § 18.2-386.2(A) (2024).

technology older than generative AI, but will also hopefully be broad enough to cover technologies that follow generative AI.

4. No Specific Intent Requirements

Furthermore, federal legislation should not require that perpetrators act with specific intent, such as to harass, humiliate, or cause emotional distress. To encourage the prosecution of deepfake pornography, the legal system should avoid imposing these requirements, which create significant barriers for victims seeking justice. Instead, the criminalization of "intentional" disclosures of deepfake pornography should take Minnesota's approach. Instead of requiring malicious intent for criminal liability, this approach focuses on purposeful disclosures and provides harsher penalties for deepfakes that were disseminated with malicious intent.[277]

5. No Disclaimer Loophole

Federal legislation should not include any requirement that the deepfake be so realistic that a reasonable person would believe it to be authentic. Such an approach leaves a large loophole for perpetrators of lower-quality deepfakes or deepfakes with a disclaimer to escape criminal liability.[278] Instead, federal legislation should mirror Florida's deepfake pornography law and state that a disclaimer notifying viewers that the depicted individual did not consent or participate in the creation of the material "is not a defense and does not relieve a person of criminal liability."[279]

6. Exceptions for Public Policy

Federal legislation should also follow the majority of states and provide limited exceptions for public policy purposes, such as law enforcement, legal proceedings, reporting, and medical treatment. These exceptions would encourage viewers and victims to report the deepfake material and seek appropriate resources to get help.

7. No Expansion of Section 230 Protections

Arguably, the most compelling reason to enact federal criminal legislation on deepfake pornography is to close the loophole that Section 230 provides for online service providers.[280] Although federally prosecuting individuals is a good start to combating deepfake pornography, it would not be as efficient or effective as prosecuting platforms that host and help disseminate deepfake pornography. Unlike for state law violations, Congress specifically included an exception to Section 230 immunity for federal criminal law violations.[281] Since states are unable to do so, federal legislation on deepfake pornography should take advantage of this exception and avoid expanding Section 230 immunity.

---

277. *See* MINN. STAT. § 617.262(3) (2023).
278. *See* Pascale, *supra* note 60, at 345.
279. FLA. STAT. § 836.13(4) (2022).
280. *See supra* Section II.A.
281. 47 U.S.C. § 230(e)(1).

8. Civil Right of Action

Federal legislation on deepfake pornography should also provide for a civil right of action for victims in addition to criminalizing the disclosure of deepfake pornography. Although a civil remedy alone would not provide the best legal recourse for victims because of the issues of finding and obtaining a judgment from a perpetrator,[282] federal legislation should not close the door for victims who want to pursue civil action. After all, civil litigation does provide benefits to plaintiffs, such as a lower burden of proof, more control throughout the case, recovery of monetary damages, and increased privacy measures during litigation.[283]

CONCLUSION

Deepfake pornography is a violence-against-women issue that has reached the hands of the general public in recent years due to the accessibility and ease-of-use of generative AI. Deepfake pornography, stemming from sexual privacy and nonconsensual pornography, represents the latest method of sexually exploiting women. Victims are left with little legal recourse—perpetrators may evade liability due to anonymity and jurisdictional challenges, and Section 230 provides immunity for the platforms that further the harms caused by deepfake pornography. As a result, traditional legal avenues, such as tort law, intellectual property law, and state nonconsensual pornography statutes, provide imperfect solutions for victims of deepfake pornography. Among the few state laws on deepfake pornography, victims' protections and requirements vary depending on where they are in the country, and victims still face the impassable barriers that Section 230 presents.

With nonconsensual pornography laws and state deepfake pornography laws to inform it, Congress should pass federal criminal legislation that applies clearly, uniformly, and efficiently across the country. Congress is in a unique position in that it has the power to sidestep the bar that Section 230 presents victims of deepfake pornography, and it should do so through enacting federal criminal legislation. Specifically, federal legislation should include: (1) clearly defined elements of the crime, (2) a broad definition of nudity, (3) a broad definition of deepfake, (4) no specific intent requirements, (5) no disclaimer loophole, (6) exceptions for public policy, (7) no expansion of Section 230 protections, and (8) a civil right of action. Such legislation will provide past, present, and future victims of deepfake pornography with the justice they deserve.

282. *See supra* Section II.A.
283. *Civil Remedies*, *supra* note 203.

***