DEEPFAKES AND INTIMATE PARTNER VIOLENCE: THE TAKE IT DOWN ACT AND OTHER PROPOSED FEDERAL LEGISLATION

*LEOR Z. ROSEN**

TABLE OF CONTENTS

* J.D., New York University School of Law, Class of 2026; B.A., University of Michigan, Class of 2020. I would like to thank the editors of the NYU Annual Survey of American Law for their thoughtful feedback and edits; Professor Emily Sack for a meaningful semester in NYU's Domestic Violence Seminar and for her guidance during the writing process; image-based technology abuse expert Carrie Goldberg for her critical insights; and my family and friends for their unwavering support. Most importantly, I am indebted to the countless survivors whose strength and resilience have inspired me to pursue this work, write this piece, and dedicate my career to the law.

I.
INTRODUCTION

Jane[1] was in an emotionally abusive relationship for two years. After multiple attempts to break up with her abusive boyfriend, who threatened to commit suicide if she left him, she was finally able to break ties—or so she thought. Two weeks later she got a message from her ex-boyfriend, stating "if you don't get back together with me, I will release this video of you." Jane was horrified when she opened the video. Despite having never taken an explicit photo or video before, the video realistically depicted Jane engaging in sexual conduct and attached her face to the body of someone performing sexual acts. Jane was distraught and worried about the potential consequences to both her career and private life. She begged her ex-boyfriend not to release the photos and scheduled an appointment to meet with a lawyer. However, early the next morning she received a text from her friend telling her to stay offline. Her ex-boyfriend had already posted the fake video with her name attached to multiple social media sites. Shortly after, she was inundated with messages from friends and family who were shocked to see "her" in a pornographic video. She was also searching for a job and had multiple interviews scheduled over the next few weeks, but she suddenly received cryptic emails rescinding her interview offers. Jane contacted multiple websites to take down the content, but it seemed like as soon as she got in touch with one platform, the same

1. Jane's story is constructed based on common situations that victims of nonconsensual sexual deepfakes face.

video popped up somewhere else. One year later, Jane is still unable to get a job and suffers from extreme anxiety and depression. The video remains online on multiple platforms, despite her continuous efforts to get them removed.

Jane's experience is representative of a cruel and troubling trend: the creation of nonconsensual sexual deepfakes to victimize both strangers and intimate partners. Deepfake technology uses artificial intelligence and learning algorithms to create deceptive content, including videos and images that give the appearance of an individual doing or saying things that they never actually did.[2] The most common type of deepfakes are nonconsensual sexual deepfakes, which are created by compiling images/videos of an intended target and then using deepfake technology to convert those images/videos into a realistic, but fake, intimate or sexual image/video.[3] Survivors of intimate partner violence ("IPV") are uniquely vulnerable to nonconsensual sexual deepfakes since the technology is easily available and intimate abusers are opportunistic offenders who have access to numerous photos of their intimate partners. Since internet content is notoriously difficult to permanently remove, abusers now have access to tools to exert power and control over former intimate partners long after their relationship ends. Nevertheless, little attention has been paid to the unique harms that nonconsensual sexual deepfakes pose to survivors of IPV. Further, while some states have passed laws targeting the creation and dissemination of nonconsensual sexual deepfakes, until recently, federal legislation was elusive.[4] But federal inertia shifted on May 19, 2025, with the enactment of the TAKE IT DOWN Act—a law criminalizing the publication of intimate visual depictions, including nonconsensual sexual deepfakes, and incentivizing internet platforms to combat nonconsensual sexual deepfakes by instituting a 48-hour take down requirement after notification.[5] The Act did not, however, create a civil cause of action. This Note analyzes current state laws, the newly enacted TAKE IT DOWN Act, and other proposed federal legislation addressing nonconsensual sexual deepfakes, and it fills

2. Kweilin T. Lucas, *Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology*, 17 Victims & Offenders 647, 648–49 (2022).

3. *Id.* at 649.

4. *See infra* Part II.

5. Barbara Ortutay, *President Trump Signs Take It Down Act, Addressing Nonconsensual Deepfakes. What is It?*, Associated Press (May 20, 2025), https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615 [https://perma.cc/NB8D-GJYA].

a gap in the literature on the relationship between nonconsensual sexual deepfakes and IPV.

Part II describes the rise of deepfake technology, Part III explains why survivors of IPV are particularly susceptible to nonconsensual sexual deepfakes, Part IV details the current laws combating this trend, Part V surveys current attempts to federally regulate nonconsensual sexual deepfakes, Part VI critiques the recently passed TAKE IT DOWN Act and pending DEFIANCE Act, and Part VII suggests key takeaways for regulating nonconsensual sexual deepfakes going forward.

This Note concludes that the recently passed TAKE IT DOWN Act and pending DEFIANCE Act, while not flawless, are positive steps in protecting victims, particularly given limitations to platform liability under the First Amendment and Section 230.[6] Going forward, legislation should (1) maintain a balance between broad and narrow language to accommodate for evolving technology while ensuring that deepfake technology is specifically covered, (2) be narrowly tailored to ensure the law is not overreaching, but at the same time ensure that punishing the behavior is not too difficult, (3) punish threats to release nonconsensual sexual deepfakes, and (4) preserve the privacy of survivors by permitting anonymous filings and strict discovery requirements. Further, lawmakers should explore ways to hold platforms accountable for the creation and proliferation of deepfakes.

II.
THE RISE OF DEEPFAKE TECHNOLOGY

Deepfake technology uses "deep learning algorithms to create compelling and often deceptive media content, such as videos, audio recordings, or images, that appear to feature real people saying or doing things they never did."[7] Researchers first introduced the technology in 2016, believing it would "pave the way for many new and exciting applications in the fields of VR/AR, teleconferencing, or on-the-fly dubbing of videos with translated audio."[8] Indeed, the technology has been used in a number of positive ways, including to improve films, regenerate voices for those who are unable to speak,

6. Communications Decency Act, 47 U.S.C. § 230 (providing broad immunity for internet platforms that host third-party content); *see infra* Part IV.B.

7. *2023 State of Deepfakes*, Sec. Hero (2023), https://www.securityhero.io/state-of-deepfakes/ [https://perma.cc/W85V-RNX2].

8. Justus Thies et al., *Face2Face: Real-time Face Capture and Reenactment of RGB Videos,* 62 Commc'ns of the ACM 96, 103 (2018).

translate speech and facial movements on video calls, mask the identities of those testifying in court, and expand interactive artistic experiences.[9]

However, the most popular use of the technology is for the nefarious and harmful creation of nonconsensual sexual deepfakes (also known as deepfake pornography), which are "doctored pornographic images and videos featuring one person's face believably mapped onto a body engaged in sexually explicit acts."[10] Nonconsensual sexual deepfakes first appeared online in late 2017 by a Reddit user under the name "deepfake," who posted fabricated sexual deepfakes of various female celebrities.[11] By January 2018 another Reddit user built an application to automate the deepfake creation process, which rapidly built a following of 90,000 users.[12] Today, nonconsensual sexual deepfakes makes up 98 percent of deepfake videos online.[13]

Deepfakes are particularly dangerous because the technology is widely accessible and does not require any technical expertise.[14] This gives anyone the ability to "easily generate digitally altered and deepfake images of celebrities, people they know, or anyone whose imagery they can access."[15] In fact, anyone can create nonconsensual sexual deepfakes if they have access to a few photos or videos of the intended target. These photos or videos can feature the subject doing *anything*, as the image does not need to be sexual in nature to be converted into a nonconsensual sexual deepfake. Deepfakes are a unique form of image-based abuse since "anyone can become

9. Lucas, *supra* note 2, at 649.

10. Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 Fordham L. Rev. 887, 889–90 (2019).

11. Lucas, *supra* note 2, at 650.

12. Alex Hern, *My May-Thatcher Deepfake Won't Fool You but Its Tech May Change the World*, Guardian (Mar. 12, 2018), https://www.theguardian.com/technology/2018/mar/12/may-thatcher-deepfake-face-swap-tech-change-world [https://perma.cc/82FL-XA77].

13. Sec. Hero, *supra* note 7.

14. *See* Lucas, *supra* note 2, at 647 ("There is a wide availability of software that can be used to create deepfake videos with ease, so users of this sophisticated technology do not need to have a great deal of technical skills or computer knowledge to generate videos."); Haley Reissman, *What Is Deepfake Porn and Why Is It Thriving in the Age of AI?*, U. Penn. Annenberg Rsch. (Jul. 13, 2023), https://www.asc.upenn.edu/news-events/news/what-deepfake-porn-and-why-it-thriving-age-ai [https://perma.cc/36E2-VVM3] ("Anyone can create their own deepfake porn images, regardless of their skill level, using websites with deepfake generators.").

15. Asher Flynn et al., *Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse*, 62 Brit. J. Criminology 1341, 1342 (2022).

a victim of non-consensual pornography without there ever having been a compromising image to begin with."[16] In contrast, other types of image-based abuse involve the non-consensual release of intimate photos which were originally taken consensually.[17]

Women are the most common target of nonconsensual sexual deepfakes[18] and the deepfake "algorithms are typically trained on images of women."[19] In reaction to this phenomenon, one professor suggested that women be cognizant of who can access their personal photographs since they could be used against them.[20] This suggestion is eerily reminiscent of victim-blaming language that implies women should monitor what they drink and wear to prevent sexual violence, rather than center blame and reform efforts on the perpetrators of violence. Research shows that the risk of experiencing victimization by deepfake technology is intensified for historically marginalized populations, including those living with disability, members of the LGBTQIA community, and racial minorities.[21] Unsurprisingly, survivors of nonconsensual sexual deepfakes suffer from severe mental health consequences. A study by the Cyber Civil Rights Initiative "found that 93% of victims who have been targeted by non-consensual pornography have suffered significant emotional distress."[22] Of that same study's sample population, 41% contemplated suicide, and "51% had suicidal thoughts that related to their victimization."[23]

Although the vast majority of deepfake technology is used to create nonconsensual sexual deepfakes, the public conversation surrounding deepfake technology until more recently has primarily focused on its threat to elections, businesses, and national security.[24] However, the use of nonconsensual sexual deepfakes has increasingly garnered more attention. In 2019, Virginia became the first state to enact law against nonconsensual intimate deepfakes.[25] Since then,

16. Lucas, *supra* note 2, at 652.
17. *Id.* at 651–52.
18. Sec. Hero, *supra* note 7.
19. Reissman, *supra* note 14.
20. Lucas, *supra* note 2, at 654.
21. Flynn et al., *supra* note 15, at 1342.
22. Lucas, *supra* note 2, at 652 (citing *Revenge Porn Statistics*, Cyber C.R. Initiative, https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf [https://perma.cc/LM2L-RPP5]).
23. *Id.* (citing *Revenge Porn Statistics*, *supra* note 22).
24. *Id.* at 649.
25. *Combatting Sexual Deepfakes: States Address the Alarming Proliferation of Nonconsensual Sexual Deepfakes*, Multistate.ai, Multistate.ai/deepfakes-sexual [https://perma.cc/QQ8V-GMAT].

30 states have followed suit.[26] In January 2024, the fervor to combat this behavior was reignited when sexually explicit deepfake images of Taylor Swift were released on the internet.[27] Notably, after the Swift pictures were released, a cyber security expert questioned how teenagers can protect themselves online if a prominent public figure such as Taylor Swift is unable to do so.[28]

While the most widely circulated and viewed deepfake technology videos are often of celebrities, "[t]he vast majority of people using these [tools] want to target people they know."[29] As such, deepfake technology poses significant risks for survivors of intimate partner violence.[30]

III.
IPV SURVIVORS ARE UNIQUELY VULNERABLE TO NONCONSENSUAL SEXUAL DEEPFAKES

Survivors of intimate partner violence ("IPV") are particularly susceptible to nonconsensual sexual deepfakes. IPV is a "pattern of abusive behavior in any relationship that is used by one partner to gain or maintain power and control over another intimate partner" and can involve "physical, sexual, emotional, economic, psychological, or technological actions or threats of actions or other patterns of coercive behavior that influence another person within an intimate partner relationship."[31] Since abusers are opportunistic

26. *Id.* (Alaska, Arkansas, Connecticut, Kansas, Maine, Maryland, Michigan, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Dakota, Ohio, Oregon, Rhode Island, South Carolina, West Virginia, and Wyoming have still *not* enacted a single bill regulating nonconsensual sexual deepfakes.).

27. *See* Ian Krietzberg, *A Whole New World: Cybersecurity Expert Calls Out the Breaking of Online Trust*, TheStreet (Mar. 25, 2024, 8:00 PM), https://www.thestreet.com/technology/a-whole-new-world-cybersecurity-expert-calls-out-the-breaking-of-online-trust [https://perma.cc/LR32-XXA4].

28. *Id.* ("If Taylor Swift can't protect herself online, how can our teenagers?" (quoting cyber security expert Masha Sedova, Vice President of Human Risk Strategy at Mimecast)).

29. Jesselyn Cook, *A Powerful New Deepfake Tool Has Digitally Undressed Thousands of Women*, Huffington Post (Nov. 8, 2021, 12:50 AM) (first alteration added) (quoting deepfake expert Henry Ajder), https://www.huffpost.com/entry/deepfake-tool-nudify-women_n_6112d765e4b005ed49053822 [https://perma.cc/EH9N-LWEU].

30. *See generally*, Lucas, *supra* note 2, at 648 ("Domestic violence victims are especially vulnerable to experience technology-facilitated abuse . . . .").

31. *Domestic Violence*, U.S. Dep't of Just. Off. on Violence Against Women, https://www.justice.gov/ovw/domestic-violence [https://perma.cc/VHD3-UL4G].

offenders[32] and will employ a variety of different abusive tactics, the easily available tool of deepfake technology is another way for abusers to exert power and control over victims.[33] As one researcher remarked, "[t]hanks to deepfakes, perpetrators of violence now have a seemingly endless platform to abuse victims."[34] For example, one survivor of nonconsensual sexual deepfakes described that her partner created and shared "very hardcore [deepfake] porn" with her name and face attached.[35]

The more photos a perpetrator has of a person, the more realistic a deepfake can be.[36] IPV survivors are at particular risk because their abusers may have access to a large swath of images of them, none of which need to be sexual in nature. For example, one reddit user participating in a discussion thread on deepfakes, asked for help making a "porn video with [his] ex-girlfriend," even though he only had photos of her.[37] However, an abuser does not even need personal or exclusive access to photos of the individual in order to make a deepfake. They can simply use publicly accessible images from social media platforms and other sites that host photos such as dating apps. In a chatroom on Discord, one user shared a story of how they made a deepfake video of a girl who attended their high school using hundreds of photos from her Instagram and Facebook accounts.[38] There are also reports of Reddit threads where individuals inquired about using photos taken from social media to create deepfakes of various individuals, including of a "friend's

32. For example, the COVID-19 lockdown policies were associated with increased rates of domestic violence as abusers took advantage of the isolating nature of lockdown to terrorize their partners. Sarah M. Peitzmeier et al., *Increases in Intimate Partner Violence During COVID-19: Prevalence and Correlates*, 37 J. Interpersonal Violence NP20482 (2022); Assan Dickson, *Domestic Abuse, an "Opportunistic Infection" of Coronavirus Pandemic*, Bus. & Fin. Times Online (Apr. 11, 2020), https://thebftonline.com/2020/04/11/domestic-abuse-an-opportunistic-infection-of-coronavirus-pandemic/ [https://perma.cc/GPT4-PHU3] (describing domestic abuse as an "opportunistic infection of the coronavirus pandemic").

33. *See* Lucas, *supra* note 2, at 648 (explaining that perpetrators of nonconsensual sexual deepfakes, like perpetrators of revenge pornography and sextortion, abuse technology "to control, intimate [sic], isolate, shame, and micromanage victims . . . .").

34. *Id.* at 652.

35. Flynn et al., *supra* note 15, at 1346.

36. Sara H. Jodka, *Manipulating Reality: The Intersection of Deepfakes and the Law*, Reuters (Feb. 1, 2024), https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01/ [https://perma.cc/KGH7-43S8].

37. Samantha Cole, *People Are Using AI to Create Fake Porn of Their Friends and Classmates*, Vice (Jan. 26, 2018), https://www.vice.com/en/article/ai-fake-porn-of-friends-deepfakes/ [https://perma.cc/S324-YS7P].

38. *Id.*

stepmom," a "coworker of mine." a "college friend," "a friend of mine and my crush," and the "hottest girl in engineering."[39]

Abusers will sometimes threaten to distribute deepfake technology "to victims' family, friends, employers, prospective employers, coworkers, and peers."[40] While threats to distribute can be deeply harmful to victims, the law often fails to cover this behavior. For example, the current New York Law targeting dissemination or publication of intimate images does not cover threatening behavior, which has proved harmful to accountability efforts.[41]

Survivors of IPV have reported that their partners' motivations for creating nonconsensual intimate deepfakes were rooted in desires for "control, power, revenge and sexual gratification."[42] As one survivor explained: "I was his first girlfriend and he very much put me on a pedestal and then when we weren't together forever, he was very, very angry, and then it went obviously to the other extreme and I was the spawn of Satan. . . . He very much dehumanised [sic] me. . . . I do think [the nonconsensual sexual deepfake] was revenge and he felt that I needed punishing."[43]

Since photos on the internet are difficult to permanently remove, survivors face the fear of the deepfake resurfacing at any moment, and as such, abusers have access to a technological tool to exert power and control against former intimate partners long after their relationship ends. This is particularly difficult for victims of non-consensual sexual deepfakes, and image-based abuse more generally, since their main goal is often "for their images to be taken off the Internet."[44]

Further, IPV survivors who are victimized by deepfake technology may continue to experience further abuse and re-traumatization when reporting the nonconsensual sexual deepfake. One survivor of nonconsensual sexual deepfakes remarked: "[s]peaking about

39. *Id.*

40. Lucas, *supra* note 2, at 652.

41. *See* N.Y. Penal Law § 245.15 (McKinney 2025); People v. Beausejour, No. CR-038513-23KN, 2024 NYLJ LEXIS 2303 (N.Y. Crim. Ct. July 18, 2024) (threatening to disseminate intimate images of an ex-girlfriend if she "continued to refuse [him]" was not found to establish an intent to cause harm).

42. Flynn et al., *supra* note 15, at 1351.

43. *Id.*

44. *See* Kara Kelleher, *Revenge Porn and Deep Fake Technology: The Latest Iteration of Online Abuse*, Dome (Aug. 10, 2023), https://sites.bu.edu/dome/2023/08/10/revenge-porn-and-deep-fake-technology-the-latest-iteration-of-online-abuse/ [https://perma.cc/5E3S-EWHX]; Telephone Interview with Carrie Goldberg, Attorney, C.A. Goldberg (Oct. 29, 2024) (notes on file with author) (explaining that many victims of image-based abuse just want the images to be taken down and to move on with their lives without having to engage the penal or civil system).

this stuff opens the door for more abuse . . . [and] every time you do it, you have to relive the thing over again."[45] Even worse, law enforcement may not treat these egregious acts with the attention they deserve. Studies show that victims believe criminal justice workers will treat non-consensual acts that occur in the digital setting as less serious than other forms of abuse.[46] Further, even if the images are successfully removed from the internet, the reputational and emotional damage is already done.[47] The difficulty of removing these images and the lack of appropriate legal recourse has demoralized and disenchanted even the most powerful of people. After a nonconsensual sexual deepfake surfaced of actress Scarlett Johansson, she told the Washington Post that she thinks litigation is "a useless pursuit."[48]

Since there is a dearth of research regarding the intersection of IPV and nonconsensual sexual deepfakes and the technology is still relatively new, the exact percentage of deepfakes that target intimate partners is unknown.[49] Since celebrities have the most widely available images online, nonconsensual sexual deepfakes depicting celebrities are likely the most prominent form of deepfakes. However, this could change. Carrie Goldberg, a prominent image-based technology abuse expert and attorney, said in an interview that, while her cases involving intimate partners still revolve around the non-consensual sharing of *consensual* photography, and not deepfake images/videos, the world of people working in the image-based abuse space are "bracing for impact."[50] Goldberg explained that she sees nonconsensual deepfake image-abuse as a threat of what is ahead for IPV, and that given the rapidly evolving nature of

45. 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/9AB4-5S8A].

46. Lucas, *supra* note 2, at 655 (citing Bridget Harris, *Spacelessness, Spatiality and Intimate Partner Violence: Technology-facilitated Abuse, Stalking and Justice Administration*, *in* Intimate Partner Violence, Risk and Security: Securing Women's Lives in a Global World 52 (Kate Fitz-Gibbon et al. eds., 2018)).

47. *See* Delfino, *supra* note 10, at 898–99.

48. Drew Harwell, *Scarlett Johansson on Fake AI-Generated Sex Videos: 'Nothing Can Stop Someone from Cutting and Pasting My Image'*, Wash. Post. (Dec. 31, 2018), https://sites.bu.edu/dome/2023/08/10/revenge-porn-and-deep-fake-technology-the-latest-iteration-of-online-abuse/ [https://perma.cc/GX85-9747].

49. *See* Lucas, *supra* note 2, at 648 ("[R]esearch on the use of non-consensual sexual deepfakes is in its infancy.").

50. Telephone Interview with Carrie Goldberg, Attorney, C.A. Goldberg (Oct. 29, 2024) (notes on file with author).

technology, such abuse could become a more common problem at any moment.[51]

Deepfake technology is not going anywhere. The technology continues to evolve and advance.[52] In addition, its popularity continues to increase. In the last five years, the number of nonconsensual sexual deepfake videos available online has increased ninefold, and monthly traffic to top deepfake sites between 2020 and 2023 increased by 285 percent.[53] Thus, now is a critical time to ensure proper regulation of this technology, hold those who abuse the technology accountable, deter further nefarious use, and protect those most vulnerable to deepfake abuse, including survivors of intimate partner violence.

IV.
PRIOR ATTEMPTS TO COMBAT NONCONSENSUAL SEXUAL DEEPFAKES

When nonconsensual sexual deepfakes began proliferating on the internet, it became clear that the laws targeting image-based abuse needed to be amended to account for this emerging form of harm. While revenge pornography laws are rooted in a violation of the right to sexual privacy, the same right does not exist regarding deepfakes, because deepfakes "arguably do not depict a person who exists"[54] and it is "not the victim's own nudity depicted in the videos."[55] The same logic makes it difficult to argue that nonconsensual sexual deepfakes are a violation to rights of publicity.[56]

As such, many states have endeavored and been successful in passing laws on nonconsensual sexual deepfakes.[57] However, the relief offered for survivors significantly varies across jurisdiction and some survivors have no options for recourse. Thus, it is essential that nonconsensual sexual deepfakes are federally regulated. However, historically, federal legislation has been doomed by First Amendment and Section 230 concerns.

---

51. *Id.*

52. Lucas, *supra* note 2, at 647–48. *See generally* Sec. Hero, *supra* note 7.

53. Cecilia D'Anastasio & Davey Alba, *Google and Microsoft Are Supercharging AI Deepfake Porn*, Bloomberg (Aug. 24, 2023), https://www.bloomberg.com/news/articles/2023-08-24/google-microsoft-tools-behind-surge-in-deepfake-ai-porn [https://perma.cc/TQA9-BURV].

54. Delfino, *supra* note 10, at 897.

55. Lucas, *supra* note 2, at 655.

56. *See* Benjamin T. Suslavich, Note, *Nonconsensual Deepfakes: A "Deep Problem" for Victims*, 33 Alb. L.J. Sci. & Tech. 160, 175–76 (2023).

57. Multistate.ai, *supra* note 25.

A. State Efforts Have Been Successful, but Coverage Significantly Varies by Jurisdiction

In 2019, Virginia became the first state to address nonconsensual sexual deepfakes and California, Hawaii, and Georgia followed suit over the next two years.[58] To date, "30 states have enacted laws addressing sexual deepfakes," and "[o]f those laws, 21 restrict the distribution of nonconsensual sexual deepfakes, 20 prohibit creation of AI-generated CSAM [child sexual abuse material], and 13 states have addressed both."[59] While the passage of these laws indicates that many states are striving to combat nonconsensual sexual deepfakes, the coverage and requirements of each statute greatly vary across jurisdiction, leaving some survivors with limited or no recourse. Some states require an intent to cause harm which can be very difficult to prove, particularly if the creator of the deepfake had other motives such as "money, attention, or clout."[60] In addition, some states only have a civil right of action, others only impose criminal penalties, and some have both.[61] Further, some state laws fail to address jurisdictional issues which can make it difficult for criminal or civil penalties to be enacted.[62] This means that if the proper jurisdiction for a legal claim does not penalize the abuse of deepfakes, a nonconsensual sexual deepfake survivor will be left without recourse, including an inability to seek an order of protection on the basis of that behavior.[63] For example, egregious

58. *Id.*

59. *Id.* Interestingly, there does not seem to be any public filings or decisions that implicate the deepfake portion of these laws. The reason for the lack of filings under this statute is unclear, since no research to date has identified this trend. Possible explanations include the fact that many of these statutes are relatively new, deepfake cases are still predominantly impacting celebrities who do not want to move forward legally or prefer to settle matters privately, and victims may desire to remain anonymous or be unwilling to file because of the time and money involved in bringing a civil claim.

60. Lucas, *supra* note 2, at 653, 655.

61. *See generally* Delfino, *supra* note 10.

62. *See* Lucas, *supra* note 2, at 653.

63. In New York, for example, to receive an order of protection, the offending individual must have either committed a family offense, which are often based on penal laws, or committed a crime. *Orders of Protection*, Off. for the Prevention of Domestic Violence, https://opdv.ny.gov/orders-protection [https://perma.cc/HUW5-TPSP]. Now that New York has amended its penal law on unlawful dissemination or publication of intimate images to include images created or altered by digitization, N.Y. Penal Law § 245.15 (McKinney 2025), the dissemination or publication of intimate nonconsensual deepfakes now qualifies as a family offense on the basis of which an order of protection can be granted. N.Y. Fam. Ct., *Family Offense Petition Form* 1 (2020) [https://perma.cc/NJ29-YHEB].

abuse of deepfake technology to victimize multiple individuals will go unpunished in states that do not criminalize nonconsensual sexual deepfakes. In 2023, a man targeted eleven different women from his high school by using deepfake technology to alter their social media photos into sexually explicit images.[64] He posted these nonconsensual sexual deepfakes on porn sites, "shared the women's personal identifying information, including full names, phone numbers and addresses—and encouraged other users on the porn site to harass and threaten them with violence."[65] Despite his deplorable actions, prosecutors were unable to charge the perpetrator for the extent of his behavior, since New York did not yet have a law criminalizing nonconsensual sexual deepfakes.[66] In the end, he was sentenced to a mere six months in jail, and that was only because one of the images depicted a minor.[67] This behavior must be federally regulated because the uneven coverage of state laws makes it difficult to properly punish this harmful behavior and leaves some survivors without an avenue of redress.

B. Until Recently, Federal Efforts Have Failed

Despite the importance of federally regulating nonconsensual sexual deepfakes, previous attempts to pass federal civil and criminal laws on deepfakes have, until recently, been unsuccessful, largely due to First Amendment freedom of speech concerns and Section 230 of the Communications Decency Act ("CDA"). The Supreme Court has held that false and/or offensive speech is protected by the First Amendment.[68] Further, Section 230 of the CDA broadly shields internet platforms from incurring liability for any third-party content posted on their platforms.[69] Abusers take advantage of this broad

64. Pei-Sze Cheng & Jennifer Millman, *Long Island Man Jailed in Deepfake Sex Scheme Targeting 11 Women From His High School*, NBC N.Y. (Apr. 18, 2023), https://www.nbcnewyork.com/news/local/crime-and-courts/long-island-man-jailed-in-deepfake-sex-scheme-targeting-14-women-from-his-high-school/4251661/ [https://perma.cc/7HBV-7N3F].

65. *Id.*

66. *Id.* In 2023, New York passed legislation criminalizing deepfakes. *See* MULTISTATE.AI, *supra* note 25.

67. Cheng & Millman, *supra* note 64.

68. Delfino, *supra* note 10, at 925 (citing United States v. Alvarez, 567 U.S. 709, 716 (2012)).

69. *Id.* at 899–900 (explaining that it is difficult for victims of nonconsensual sexual deepfakes to sue platforms because "courts give a high degree of deference to website hosts under Section 230." (quoting Rachel Budde Patton, Note, *Taking the Sting Out of Revenge Porn: Using Criminal Statutes to Safeguard Sexual Autonomy in the Digital Age*, 16 GEO. J. GENDER & L. 407, 423–24 (2015))).

protection against liability, often choosing to post deepfake content on social media platforms "because they offer users high levels of anonymity and are subject to free expression protections."[70]

First Amendment and CDA restrictions have continuously curbed the enactment of federal legislation regulating deepfakes. For example, the Malicious Deep Fake Prohibition Act of 2018 never received a single co-sponsor[71] and commentators worried about the overbroad nature of the Bill.[72] While some have suggested holding companies liable through the intellectual property exception of Section 230[73] and others have advocated to amend Section 230 to make an exception for deepfakes,[74] these solutions would likely encounter challenges.[75] For example, the intellectual property right to publicity only protects one's name, image, and likeness for commercial purposes, which is difficult to infer from housing nonconsensual sexual deepfakes.[76] Also, deepfake creators have argued that nonconsensual sexual deepfakes would satisfy the fair use doctrine since the original images are transformed into something new.[77] Amendments to Section 230 are unlikely; dozens of amendments to Section 230 have been introduced in the last three Congresses, but none have passed.[78] Thus, the current best solution is to pass narrowly-tailored federal laws which contain First Amendment carveouts and limit platform liability.

---

70. Lucas, *supra* note 2, at 652.

71. Kelleher, *supra* note 44.

72. *See, e.g.*, *Lawmakers Plunge into "Deepfake" War*, AXIOS (Jan. 31, 2019), https://www.axios.com/2019/01/31/lawmakers-plunge-into-deepfake-war-1548948076 [https://perma.cc/35N6-Z62M] (U. Va. Law Professor Danielle Citron noting that the Malicious Deep Fake Prohibition Act of 2018 "could scare platforms into immediately taking down everything that's reported as a deepfake—potentially deleting legitimate posts in the process.").

73. *See* Tyler von Denlinger, Note, *Protecting Personal Dignity: Advocating for A Federal Right of Publicity Against Pornographic Deepfakes*, 27 Chap. L. Rev. 247, 275–77 (2023) (proposing the Section 230 intellectual property exception as a workaround to holding platforms liable).

74. Nicholas O'Donnell, Note, *Have We No Decency? Section 230 and the Liability of Social Media Companies for Deepfake Videos*, 2021 U. Ill. L. Rev. 701, 704 (2021) (proposing Section 230 amendment).

75. *See* von Denlinger, *supra* note 73, at 276 (identifying potential roadblocks to using an intellectual property exception including a circuit split on the relationship between a state's right of publicity and Section 230).

76. Suslavich, *supra* note 56, at 175.

77. *Id.* at 174–75.

78. Peter J. Benson & Valerie C. Brannon, Cong. Rsch. Serv., IF12584, Section 230: A Brief Overview (2024) (explaining the numerous free speech considerations involved in amending Section 230).

V.
RECENTLY PASSED AND CURRENTLY PENDING FEDERAL LEGISLATION

This Part examines the DEFIANCE and TAKE IT DOWN Acts, two federal bills aimed at curbing deepfakes. The still pending DEFIANCE Act would impose civil liability on abusers while the recently passed TAKE IT DOWN Act imposes criminal liability on abusers as well as civil liability on platforms. Both Acts passed the Senate in 2024 but died at the end of the 2023–2024 legislative session.[79] Following the commencement of the 119th Congress, the TAKE IT DOWN Act was reintroduced, swiftly passed by both the House and the Senate, and was signed into law on May 19, 2025.[80] While the DEFIANCE Act has not yet been reintroduced, it remains the most recent effort to establish civil liability against individual abusers.

A. TAKE IT DOWN Act

The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (the "TAKE IT DOWN Act" or the "Act") aims to combat nonconsensual sexual deepfakes through two avenues: (1) establishing a criminal offense to hold those who publish intimate visual depictions criminally liable and (2) incentivizing internet platforms to combat nonconsensual sexual deepfakes by mandating a 48-hour take down requirement after notification.[81]

The Bill amends Section 223 of the Communications Act of 1934, 47 U.S.C. § 233.[82] The Bill passed the Senate and House on February 13, 2025, and April 28, 2025, respectively, and was signed into law on May 19, 2025.[83]

1. Criminal Provision

The criminal provision of the TAKE IT DOWN Act holds those who distribute nonconsensual intimate visual depictions criminally

79. S. 4569, 118th Cong. (as passed by Senate, Dec. 3, 2024); S. 3696, 118th Cong. (as passed by Senate, Jul. 23, 2024).

80. S. 146, 119th Cong. (2025); H.R. 633, 119th Cong. (2025); Ortutay, *supra* note 5.

81. S. 146, 119th Cong. (as passed by Senate, February 13, 2025, and by House, April 4, 2025).

82. *Id.*

83. Pub. L. No. 119-12, 139 Stat. 55 (2025); Ortutay, *supra* note 5.

liable.[84] The Bill establishes two types of offenses: those involving the publication of "authentic intimate visual depictions" and "digital forgeries."[85]

Although the term "authentic" is not expressly defined in the Act, the first offense presumably covers any intimate visual depiction that are unaltered or digitally manipulated and therefore not classified as digital forgeries. Under the Act, an intimate visual depiction, "depicts . . . the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual" or "the display or transfer of bodily sexual fluids . . . on to any part of the body of an identifiable individual . . . from the body of an identifiable individual" or "an identifiable individual engaging in sexually explicit conduct."[86] The offense criminalizes knowingly publishing an intimate visual depiction if it "was obtained or created under circumstances in which the person knew or reasonably should have known the identifiable individual had a reasonable expectation of privacy" and "is intended to cause harm" or "causes harm, including psychological, financial, or reputational harm, to the identifiable individual."[87]

The second offense, digital forgeries, is defined as "any intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual."[88] The Act criminalizes publishing a digital forgery of an adult if "the digital forgery was published without the consent of the identifiable individual" and publication "is intended to cause harm" or "causes harm, including psychological, financial, or reputational harm, to the identifiable individual."[89] The bill defines consent as "an affirmative, conscious, and voluntary authorization made by

84. Pub. L. No. 119-12, § 2, 139 Stat. 55, 55–60 (2025).

85. *Id.*

86. 15 U.S.C. § 6851. The TAKE IT DOWN Act uses the definition of intimate visual consent from the quoted provision. Pub. L. No. 119-12, § 2(h)(1)(E), 139 Stat. 55, 56 (2025). Note, while the proposed DEFIANCE Act, discussed *infra* Part V.B, aims to amend 15 U.S.C § 6581, the amendment does not alter its current definition of intimate visual depiction and thus the bills can both be passed without introducing any issues.

87. Pub. L. No. 119-12, § 2(h)(2)(A), 139 Stat. 55, 56 (2025).

88. *Id.* § 2(h)(1)(B), 139 Stat. at 55.

89. *Id.*§ 2(h)(3)(A), 139 Stat. at 57.

an individual free from force, fraud, duress, misrepresentation, or coercion."[90]

The Act does not contain a harm requirement for offenses involving children. Publishing authentic intimate visual depictions or digital forgeries depicting a child are punished when the intent is to "abuse, humiliate, harass, or degrade the minor" or "arouse or gratify the sexual desire of any person."[91]

The offenses both carry a possibility of a fine and/or up to 3 years of imprisonment if involving a minor or up 2 years if not.[92] The TAKE IT DOWN Act also criminalizes threats to publish both authentic intimate visual depictions and digital forgeries "for the purpose of intimidation, coercion, extortion, or to create mental distress."[93] Threats involving intimate visual depictions are punished similarly to the offense itself, and threats involving digital forgeries carry the possibility of a fine and/or up to 30 months of imprisonment if involving a minor, or up 18 months of imprisonment if not.[94]

Notably, the Bill states: "the fact that the identifiable individual provided consent for the creation of the intimate visual depiction shall not establish that the individual provided consent for the publication of the intimate visual depiction."[95]

2. Take Down Provision

The statement announcing the Senate's TAKE IT DOWN Act characterized civil action as insufficient, describing it as "time-consuming [and] expensive", a method of recourse that "may force victims to relieve trauma," and "impractical."[96] As an alternative to civil litigation, the TAKE IT DOWN Act requires that within a year of the law's enactment, May 19, 2026, every covered platform[97] shall establish a process where an individual or an authorized

90. *Id.* § 2(h)(1)(A), 139 Stat. at 55.
91. *Id.* §§ 2(h)(2)(B), 2(h)(3)(B), 139 Stat. at 56–57.
92. *Id.* § 2(h)(4), 139 Stat. at 58.
93. *Id.* § 2(h)(6), 139 Stat. at 58–59.
94. *Id.*
95. *Id.* § 2(h)(5)(A), 139 Stat. at 58.
96. Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Sens. Cruz, Klobuchar, Reps. Salazar, Dean Continue Fight to Pass TAKE IT DOWN Act, (Jan. 16, 2025), https://www.commerce.senate.gov/2025/1/sens-cruz-klobuchar-reps-salazar-dean-continue-fight-to-pass-take-it-down-act [https://perma.cc/J4SG-R3MC].
97. "Covered platform" is defined as "a website, online service, online application, or mobile application . . . that serves the public; and . . . that primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files; or . . . for which it is in the regular course of trade or business of the website, online service, online application, or mobile application to

representative can notify the platform of the presence of an intimate visual depiction published without the depicted person's consent and submit a request to remove the depiction.[98] Following a notification and removal request, the platform "shall, as soon as possible, but not later than 48 hours after receiving such request . . . remove the intimate visual depiction and make *reasonable* efforts to remove any known identical copies of such depiction."[99] The Act limits liability based on good faith efforts to remove the content.[100] Violations are enforced by the Federal Trade Commission and are treated as a violation of § 18(a)(1)(B) of the Federal Trade Commission Act, which defines unfair or deceptive acts or practices.[101] Platforms can face civil penalties of up to $50,120 per violation.[102] It is unclear how much of this money will go to victims; however, the FTC advertises that that whenever possible, it uses the money collected from defendants to provide refunds to injured consumers and pay corresponding administrative costs.[103]

A press release on the Senate's TAKE IT DOWN Act emphasized that the Act is narrowly tailored to avoid "chilling lawful speech."[104] Likely in response to First Amendment and Section 230 concerns, the Act requires that a reasonable person would view the deepfake as "indistinguishable from an authentic visual depiction of the individual."[105] Despite First Amendment concerns, Senator Shelley

---

publish, curate, host, or make available content of nonconsensual intimate visual depictions." Pub. L. No. 119-12, § 4(3)(A), 139 Stat. 55, 61 (2025).

98. *Id.* § 3(a)(1)(A), 139 Stat. at 59–60.

99. *Id.* § 3(a)(3), 139 Stat. at 60 (emphasis added).

100. *Id.* § (3)(a)(4), 139 Stat. at 60 ("A covered platform shall not be liable for any claim based on the covered platform's good faith disabling of access to, or removal of, material claimed to be a nonconsensual intimate visual depiction based on facts or circumstances from which the unlawful publishing of an intimate visual depiction is apparent, regardless of whether the intimate visual depiction is ultimately determined to be unlawful or not.").

101. *Id.* § 3(b)(1), 139 Stat. at 61.

102. *Id.* § 3(b); *Notice of Penalty Offenses*, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/penalty-offenses [https://perma.cc/AN4A-CJ4W].

103. *How the FTC Provides Refunds*, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/ftc-refund-programs/how-ftc-provides-refunds [https://perma.cc/DTQ9-HWJA].

104. Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Sen. Cruz's TAKE IT DOWN Act Clears Commerce Committee, (July 31, 2024), https://www.commerce.Senate.gov/2024/7/sen-cruz-s-take-it-down-act-clears-commerce-committee [https://perma.cc/7DN4-97VZ].

105. Pub. L. No. 119-12, § 2(h)(1)(B), 139 Stat. 55 (2025).

Moore Capito, one of the Bill's co-sponsors, emphasized the need to hold social media platforms accountable.[106]

B. DEFIANCE Act

The Disrupt Explicit Forged Images and Non-Consensual Edits Act (the "DEFIANCE Act"), would give deepfake victims a civil right of action to sue those who distribute or produce "intimate digital forgeries."[107] It seeks to amend 15 U.S.C. § 6851, the civil statute establishing an action related to disclosure of intimate images.[108] The 2024 DEFIANCE Act was introduced in the Senate by Senator Richard Durbin (D-IL) in January 2024. According to Senator Durbin, the DEFIANCE Act "was carefully crafted to comply with the First Amendment."[109] Thus, despite the First Amendment concerns which had previously curbed attempts to federally regulate deepfakes,[110] the Senate passed the Bill on July 23, 2024.[111] The 2024 House version was introduced by Representative Alexandria Ocasio-Cortez in March 2024 and was pending in the House Committee on the Judiciary before dying at the end of the legislative session.[112] The Act has yet to be reintroduced in the 119th congressional session.

In an interview, a Senate Judiciary Committee Aid explained that the purpose of the Act is to address and deter nonconsensual sexual deepfake behavior both between strangers and individuals who know each other.[113] The Senate version lays out a series of findings, including recognizing that "[d]igital forgeries are often used to—(A) harass victims, interfering with their employment,

106. Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Sen. Cruz Leads Colleagues in Unveiling Landmark Bill to Protect Victims of Deepfake Revenge Porn, (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 [https://perma.cc/825C-8TKG].

107. S. 3696, 118th Cong. §§ 3(a)(2), 3(b)(1) (as passed by Senate, July 23, 2024).

108. S. 3696, 118th Cong. § 3(a) (as passed by Senate, July 23, 2024).

109. 170 Cong. Rec. S4040 (daily ed. June 12, 2024) (statement of Sen. Richard Durbin).

110. *See supra* Part IV.B. Indeed, the same First Amendment concerns which stalled progress in the past, were present in floor debates on the DEFIANCE Act. In response to the Bill, Senator Cynthia Lummis remarked that "[t]he expansive definitions and wide net of liability in this bill could lead to unintended consequences that stifle American technological innovation and development." 170 Cong. Rec. S4040 (daily ed. June 12, 2024) (statement of Sen. Cynthia Lummis).

111. S. 3696, 118th Cong. (as passed by Senate, July 23, 2024).

112. H.R. 7569, 118th Cong. (as introduced in the House, Mar. 6, 2024).

113. Telephone interview with Senate Judiciary Committee Aid (Dec. 3, 2024) (notes on file with author).

education, reputation, or sense of safety; or (B) commit extortion, sexual assault, *domestic violence*, and other crimes."[114] The findings also recognize the "profound[] harm" caused by intimate digital forgeries, explaining that they can destabilize victims, cause feelings of helplessness and fear of being in public, and lead to depression, anxiety, and suicidal ideation.[115] The findings indicate an awareness that nonconsensual sexual deepfakes are used to commit domestic violence.[116]

Both the Senate and House versions begin by defining the technology covered by the Bill, rather broadly. The Bills seek to address "digital forger[ies]" meaning "any intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual."[117] The Bills also lay out three different causes of action that the identifiable subjects of nonconsensual digital forgeries can bring against those who disclose, produce, solicit, or possess the digital forgeries, or those who knew or recklessly disregarded that the identifiable subject had not consented to the disclosure, production, solicitation, or possession.[118] In addition, both Bills allow the court to issue a series of privacy provisions including the option to permit the plaintiff to

114. S. 3696, 118th Cong. § 2(8) (as passed by Senate, July 23, 2024) (emphasis added).

115. *Id.* § 2(3)–(7).

116. *Id.*

117. *Id.* § 3(a)(2)(D); H.R.7569, 118th Cong., § 2 (as introduced in the House, Mar. 6, 2024) (similar language).

118. *See id.* § 3(b)(1)(A); H.R.7569, 118th Cong, § 2(b)(1)(A) (2024). The first cause of action can be brought against a person who makes a "disclosure" "without the consent of the individual . . . [and] knows or recklessly disregards that the identifiable individual has not consented to such disclosure." The second cause of action can be brought "against any person that knowingly produced or possessed the digital forgery with intent to disclose it, or knowingly disclosed or solicited the digital forgery, if—(I) the identifiable individual did not consent to such production or possession with intent to disclose, disclosure, or solicitation; (II) the person knew or recklessly disregarded that the identifiable individual did not consent to such production or possession with intent to disclose, disclosure, or solicitation." The third cause of action can be brought "against any person that knowingly produced the digital forgery if (I) the identifiable individual did not consent to such production; (II) the person knew or recklessly disregarded that the identifiable individual—(aa) did not consent to such production and '(bb) was harmed, or was reasonably likely to be harmed, by the production." Interestingly, the (bb) clause in the third cause of action is not included in the House version.

use a pseudonym, require the parties to redact plaintiff's personal information from filings or file documents under seal, and establish protective orders for the purposes of discovery.[119] Further, the Bills also would establish a statute of limitations of up to 10 years from the date of discovery of the violation or 10 years after the identifiable individual turns 18, whichever is later.[120]

In terms of damages, the House Bill mirrors the current civil statute on disclosure of intimate images, 15 U.S.C. § 6851, which allows for recovery of equitable relief, litigation costs including reasonable attorneys' fees, and actual damages sustained by the individual *or* liquidated damages in the amount of $150,000. The House Bill did not allow for punitive damages.[121] In contrast, the Senate Bill proposed a more expansive relief regime than offered in 15 U.S.C. § 6851, by allowing for recovery of punitive damages or equitable relief, litigation costs including reasonable attorneys' fees, and actual damages *or* liquidated damages in the amount of either $150,000 or $250,000 if the claim was "committed in relation to actual or attempted sexual assault, stalking, or harassment of the identifiable individual."[122]

VI.
RECENTLY PASSED AND CURRENTLY PENDING FEDERAL LEGISLATION IS A WELCOME EFFORT TO COMBAT THE ONGOING THREAT

While not without limitations, the recently passed TAKE IT DOWN Act, and the pending DEFIANCE Act would provide survivors with much-needed options for recourse.

A. Addressing the Debate Over Civil Versus Criminal Legislation

Despite agreement among scholars, lawyers, politicians, and the public that the problem of nonconsensual sexual deepfakes must be addressed, there is no consensus on whether regulating deepfakes should be done through civil or criminal law.

However, this omission may have little meaning since the House Bill never left committee.

119. S. 3696, 118th Cong., § 3(b)(4) (2024) (as passed by Senate, July 23, 2024); H.R. 7569, 118th Cong., § 2(b)(4) (2024) (as introduced in the House, Mar. 6, 2024).

120. S. 3696, 118th Cong., § 3(b)(6) (2024); H.R. 7569, 118th Cong., § 2(b)(6) (2024).

121. H.R.7569, 118th Cong., § 2(b)(3) (2024).

122. S. 3696, 118th Cong., § 3(b)(4) (2024).

Civil litigation presents an opportunity for individuals to recover for their harms and can be empowering for survivors when seeking redress.[123] In addition, civil legislation tends to be easier to pass compared to criminal legislation since criminal laws can involve jail time.[124] However, Professor Rebecca Delfino and other scholars favor criminal accountability for a number of reasons, including: the cost of civil litigation, the unfairness of putting the onus on victims to come forward particularly given the common desire to remain anonymous, the more expansive fact-finding abilities of the government, and the ability to hold judgment-proof individuals accountable.[125] Professor Delfino further argues that criminal punishment signals the seriousness of the behavior, by "convey[ing] the view that the conduct is not trivial and that it is not only hurtful to the individual involved but also harmful and offensive to the community."[126] Criminal Justice Professor Kweilin Lucas asserts that criminal punishment could "save women's lives."[127] However, additional criminal laws will inevitably contribute to the broader issues of overcriminalization and mass incarceration.[128] Broad criminal laws run the risk of encompassing innocuous behavior, particularly in a world inundated by technology.[129]

Creating effective statutes to target this behavior is a complex feat. While combatting nonconsensual sexual deepfakes through civil laws is ideal given broader issues of overcriminalization, criminal

123. *See, e.g.*, Press Release, Kathy Hochul, Governor, New York, Governor Hochul Signs Adult Survivors Act (May 24, 2022), https://www.governor.ny.gov/news/governor-hochul-signs-adult-survivors-act [https://perma.cc/2243-239V] (New York Governor Kathy Hochul called the passage of the New York Adult Survivors Act, which granted lookback windows for sexual abuse survivors, an "important step in empowering survivors").

124. Telephone Interview with Senate Judiciary Committee Aid (Dec. 3, 2024) (notes on file with author) (explaining that Senator Durbin's office decided to work on passing a civil statute to address deepfake nonconsensual intimate imagery because it would probably encounter less pushback than a criminal statute).

125. Delfino, *supra* note 10, at 902–03.

126. *Id.*

127. Lucas, *supra* note 2, at 655.

128. *See generally*, James R. Copland & Rafael A. Mangual, *Overcriminalizing America: An Overview and Model Legislation for States*, Manhattan Inst. (Aug. 8, 2018), https://manhattan.institute/article/overcriminalizing-america-an-overview-and-model-legislation-for-states [https://perma.cc/CYK9-K3WF]; Ashley Nellis, *Mass Incarceration Trends,* Sentencing Project (May 21, 2024), https://www.sentencingproject.org/reports/mass-incarceration-trends/ [https://perma.cc/VQ8L-NQDB].

129. Telephone Interview with Senate Judiciary Committee Aid, (Dec. 3, 2024) (notes on file with author) (explaining concerns regarding broad criminalization of nonconsensual sexual deepfakes since children can easily access deepfake creation tools without sufficient knowledge of the resulting harm).

liability may be needed to combat this harmful behavior given that civil liability puts the onus on survivors to file suit and the current state of the law precludes platform liability.[130] This is especially true in more serious cases involving repeat offenders or offenses against vulnerable populations such as minors. Notably, each survivor of nonconsensual sexual deepfakes may desire a different form of recourse or elect to take no action at all. Thus, it is beneficial to present survivors with an array of legal options, which in turn, can help return the agency and autonomy that was stripped from them by the deepfake abuse.

B. TAKE IT DOWN Act

1. Criminal Provision

The TAKE IT DOWN Act's criminal provision is a helpful criminal option for combatting nonconsensual sexual deepfakes. First, the broad definition of digital forgery, which covers a list of technological tools and includes a catch-all phrase of "any other [depiction created through the use of] computer-generated or technological means," accounts for the ever-changing landscape of technology.[131] Second, while remaining broad, the statute very clearly covers deepfakes, by including digital forgeries that "adapt[], modify[], manipulat[e], or alter[] an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual."[132] Third, the TAKE IT DOWN Act affirmatively punishes threatening behavior, which is an important step for protecting victims from a significant tool of power and control.[133] Fourth, the bill avoids victim-blaming language by noting "the fact that the identifiable individual provided consent for the creation of the intimate visual depiction shall not establish that the individual provided consent for the publication of the intimate visual depiction."[134] In doing so, the Act addresses the fact that the original photos used to create the non-consensual deepfake image were likely taken consensually. Fifth, the Act accounts for the difficulty in

130. *See infra* Part IV.B.

131. *See supra* Part V.A.1; 47 U.S.C. § 223(h)(1)(B). Like the TAKE IT DOWN Act, California's deepfake statute (Cal. Civ. Code § 1708.86) is "unique because it explicitly avoids using the term 'deepfake' in its text [and, instead,] . . . employs the terms 'altered depiction,' 'depicted individual,' and 'digitization.'" von Denlinger, *supra* note 73, at 262.

132. *See supra* Part V.A.1.; 47 U.S.C. § 223(h)(1)(B).

133. *See supra* Part V.A.1.

134. *Id.*; 47 U.S.C. § 223(h)(5)(A).

proving intent, by requiring either an intent to cause harm *or* that harm was caused.[135] The "harm was caused" clause accommodates for the fact that intent to cause harm is notoriously hard to prove, and that there could be circumstances in which a nonconsensual sexual deepfake was created partly for financial incentives, but still deeply harms a victim. Note that provisions regulating depictions of children appropriately do not contain a harm requirement, which accords with common consensus on the particular vulnerability of children.[136]

Notably, the Act appropriately acknowledges the lack of consent at the heart of intimate forgeries since using a non-intimate photo and artificial intelligence to create an intimate image that never happened is rarely, if ever, done with a victim's consent. While the Act's authentic intimate image violation involves a contextual inquiry around if the image was "obtained or created under circumstances in which the person knew or reasonably should have known the identifiable individual had a reasonable expectation of privacy," the intimate forgery inquiry only asks whether there was affirmative consent.[137] Using affirmative consent in the statutory language signifies that the very essence of nonconsensual sexual deepfakes, as indicated by its name, is a lack of consent. Importantly, the difference between the two does not diminish the lack of consent involved in the nonconsensual distribution of intimate images; however, it highlights that the very creation of the nonconsensual deepfakes is rooted in fabrication. Given the rarity that a sexual deepfake would be created consensually, legislators should have considered creating a rebuttable presumption of no consent when an individual has knowledge that the intimate image is a forgery. Of course, the presumption would be rebutted when there is evidence that the alleged perpetrator reasonably believed consent was given.

Overall, the TAKE IT DOWN Act's criminal remedy provides a less onerous option for survivors and could provide a major avenue of deterrence and/or accountability in situations involving repeat offenders and minors. While issues of overcriminalization remain, given the pressing need to deter this behavior and curb the

135. *See supra* Part V.A.1.

136. *Id.*

137. 47 U.S.C. §§ 223(h)(2)(A)(1), (h)(3)(A). The requirement of *affirmative* consent in this Act is admirably broader than is typical of other criminal laws addressing sexual violence. *See, e.g.*, 10 U.S.C. § 920 (no "affirmative" requirement in definition of consent); N.Y. Penal Law § 130.05 (McKinney 2025) (same); Cal. Penal Code § 261.6 (West 2025) (same). Legislatures should consider using this more expansive definition of consent in other instances.

proliferation of deepfakes as the technology evolves and improves, the TAKE IT DOWN Act's criminal provision presents an important way to fight this behavior.

2. Take Down Provision

The TAKE IT DOWN Act may provide significant motivation for companies to combat this behavior because Section 230 protections currently limit incentives for companies to implement solutions.[138] Given companies' desire to maintain positive publicity and avoid liability, the Act would hopefully lead to faster removal of deepfake images. Ensuring the help of platforms in removing deepfake content is particularly important since oftentimes the sole desire of survivors is to remove the deepfake from the internet.[139]

Some internet platforms have already independently banned deepfakes and implemented procedures for removing them, however, these procedures are not regulated, and many programs require opting in. For example, current tools titled "Take It Down" and "Stop Non-Consensual Intimate Image Abuse," provide a forum for identification of real or deepfake intimate images, which then triggers removal procedure for all participating companies. While Facebook, Instagram, TikTok, Pornhub, and OnlyFans are all participating companies, X (formerly Twitter) is not.[140] Before Elon Musk bought Twitter, the platform announced a 3-prong test to determine if a deepfake should be removed. If the content met all three factors—"Is the media synthetic or manipulated? Was it shared in a deceptive manner? Is it likely the content will cause serious harm?"—Twitter said it was "very likely to remove the content" but "refrained from making a blanket statement saying it would always do so."[141] Since Mr. Musk acquired Twitter (now X), it is unclear what its policies are. While X's current policies supposedly require deepfakes to be taken down or labeled as AI-generated, Mr. Musk

138. Lucas, *supra* note 2, at 654.

139. Kelleher, *supra* note 44; *see* Telephone Interview with Carrie Goldberg, Attorney, C.A. Goldberg (Oct. 29, 2024) (notes on file with author).

140. *See* Kelleher, *supra* note 44. *See generally Industry Partners*, StopNCII, https://stopncii.org/partners/industry-partners/?lang=en-gb [https://perma.cc/AJG3-359L]; *Participating Online Platforms*, Take It Down, https://takeitdown.ncmec.org/participants/ [https://perma.cc/JK6P-J5SH].

141. Lauren Feiner, *Twitter Unveils New Rules to Tackle Deepfakes Ahead of the 2020 Election*, CNBC (Feb. 4, 2020, 4:00 PM), https://www.cnbc.com/2020/02/04/twitter-unveils-new-rules-to-tackle-deepfakes-ahead-of-2020-election.html [https://perma.cc/T9VL-PVK6].

himself shared an AI-generated video of Vice President Kamala Harris during the 2024 Presidential Election.[142]

Thus, the TAKE IT DOWN Act could ensure baseline standardization across all covered companies and force any companies who are opting out of private enforcement tools, including X, to begin combatting the rampant issue. However, identification and removal tools notoriously have limitations. If an image is sent through an encrypted platform, such as WhatsApp, the removal procedures of the "Take It Down" tool will not be initiated.[143] Additionally, if an image is altered, including cropped or edited with a filter, a whole new submission is required to register the image as a deepfake.[144] Professor Delfino has noted that "platforms like Pornhub have been largely unsuccessful in removing current content and stopping creators from posting new content."[145]

Ideally, the TAKE IT DOWN Act would drive companies to find much-needed solutions to the limitations of these tools. However, many of the covered companies already maintain tools and procedures that may fit the "reasonable effort" and good-faith requirements of the Act such as the aforementioned "Take It Down" and "Stop Non-Consensual Intimate Image Abuse," tools. If so, the Act would spark little change. Further, since photos on the internet are difficult to permanently remove, the Act's mandated take down provision is unlikely to ensure the photos are gone forever. Even so, mandating a 24-hour take down requirement, instead of the enacted 48-hour requirement may have better addressed survivors' needs so that individuals have fewer opportunities to save or screenshot deepfakes.[146]

Critics have continued to emphasize that the Act "threatens free expression, user privacy, and due process" and would lead to "[o]verreach and [c]ensorship."[147] The Electronic Frontier

142. Press Release, Robert Weissman, Co-President, Public Citizen, X Must Take Down Harris Deepfake To Comply With Its Own Policies (July 29, 2024), https://www.citizen.org/news/x-must-take-down-harris-deepfake-to-comply-with-its-own-policies/ [https://perma.cc/YC9Y-M9H6].

143. Kelleher, *supra* note 44.

144. *Id.*

145. Delfino, *supra* note 10, at 901.

146. While a 24-hour take down mandate would lower the chances that a deepfake will be widely circulated, Congress would likely be skeptical of a shorter time frame given Section 230 protections.

147. Joe Mullin, *The TAKE IT DOWN Act: A Flawed Attempt to Protect Victims That Will Lead to Censorship*, Elec. Frontier Found. (Feb. 11, 2025), https://www.eff.org/deeplinks/2025/02/take-it-down-act-flawed-attempt-protect-victims-will-lead-censorship [https://perma.cc/T42J-MH58].

Foundation ("EFF"), a nonprofit focused on protecting civil liberties in the digital world, is particularly worried that powerful people will use this tool to take down lawful journalism and political speech.[148] President Trump validated this fear when he noted in his March 4, 2025, joint address to Congress, that he is "going to use that bill for myself too, if you don't mind . . . because nobody gets treated worse than I do online. Nobody."[149] Indeed, President Trump's comment belittles the severity of this problem and takes away the focus from victims who deserve recourse. Yet, the legislation continues to be endorsed by "over 100 organizations, including platforms such as Microsoft, Snap, and Meta [and Google]; sexual violence organizations like the Rape, Incest, and Abuse National Network and the National Center on Sexual Exploitation; and civil society organizations like SAG-AFTRA and the American Principles Project."[150] Further, the EFF provides no appropriate alternatives for holding platforms accountable, instead suggesting that the focus should be on civil liability for perpetrators and that platforms only role is to "improv[e] reporting and evidence collection systems."[151] However, since platforms play an integral role in enabling this problematic behavior and the current unregulated framework is not working, the failure to suggest effective alternatives calls the thoroughness of the critique into question.

Despite criticisms, the TAKE IT DOWN Act has become law after a rare bicameral and bipartisan effort.[152] President Trump noted in his joint address to Congress on March 4, 2025, that he "look[s] forward to signing [the TAKE IT DOWN] bill into law" after it passes the House.[153] Importantly, taking down these images does not combat the root of the problem: that deepfake technology is widely accessible and platforms allow these depictions to be housed on their websites. However, since the First Amendment and Section 230 continue to impose stringent protections for internet platforms, the TAKE IT DOWN Act may present the most practical and narrowly

148. *Id.*

149. Donald J. Trump, President of the United States, Remarks By President Trump in Joint Adress to Congress (March 4, 2025), https://www.whitehouse.gov/remarks/2025/03/remarks-by-president-trump-in-joint-address-to-congress/ [https://perma.cc/3KDW-VP4T].

150. Sunny Gandhi & Adam Billen, *The US Senate's Passage of the TAKE IT DOWN ACT Is Progress on an Urgent, Growing Problem*, Tech Pol'y Press (Feb. 21, 2025), https://www.techpolicy.press/the-us-senates-passage-of-the-take-it-down-act-is-progress-on-an-urgent-growing-problem/ [https://perma.cc/YNX8-CNZD].

151. Mullin, *supra* note 147.

152. Ortutay, *supra* note 5.

153. Remarks of Donald J. Trump, *supra* note 149.

tailored solution to addressing victims' desire and right to have nonconsensual deepfake intimate images removed.

C. DEFIANCE Act

The DEFIANCE Act is a good step in the right direction towards combatting nonconsensual sexual deepfakes through a civil right of action. First, in identical language to the TAKE IT DOWN Act, DEFIANCE accounts for the ever-changing landscape of technology, while still very clearly covering deepfakes.[154] Second, courts can employ various privacy options to better protect plaintiffs, including permitting them to file suit under pseudonym, which may assuage victims' concerns about the publicity of civil litigation.[155] Third, both the Senate and House Bills wisely employ extended statute of limitations periods (10 years from discovery or from the time you turn 18, whichever is later),[156] aligning with evidence that survivors of sexual violence may not immediately report the misconduct.[157] Fourth, the Senate version remarkably recognizes the harm that "intimate digital forgeries" have on survivors of domestic violence and sexual violence, which concretizes the fact that this technology negatively impacts marginalized populations.[158] Fifth, while both Bills seem to provide an adequate amount of deterrence for this behavior, the Senate Bill provides even stronger opportunities for survivors to seek recourse by expanding damages beyond what the current civil statutes on disclosure of intimate images provides. Specifically, the Senate Bill allows for both punitive damages and increased damages when the action is "committed in relation to actual or attempted sexual assault, stalking, or harassment of the identifiable individual."[159]

Despite its commendable qualities, there is still room for improvement.[160] Even though the Bill attempts to combat the

154. *See supra* Part V.B.; *see also supra* note 131.

155. *See supra* Part V.B.

156. *Id.*

157. *Understanding Statutes of Limitations for Sex Crimes*, RAINN, https://rainn.org/articles/statutes-limitations-sex-crimes [https://perma.cc/6J27-3FMH].

158. S. 3696, 118th Cong. § 2 (as passed by Senate, July 23, 2024).

159. *Id.* § 3(b)(4).

160. In assessing potential areas for improvement, note that one of the main goals in drafting the DEFIANCE Act was to create legislation that would pass Congress and address the lack of federal legislation *as quickly as possible*. *See* Telephone Interview with Senate Judiciary Committee Aid (Dec. 3, 2024) (notes on file with author) (explaining that fast passage of legislation was critical). Thus, strategic decisions may have been made to omit or include certain types of provisions in order to ensure the Act's quick passage.

difficulties involved in filing a civil claim by allowing the court to issue privacy protections, a court is not encouraged or required to do so. Since the issuance of privacy protections is within a court's discretion, survivors might still be deterred from seeking civil liability. To ensure a civil action is utilized, it would be helpful to amend the privacy provision to instruct courts to issue privacy protections upon the request of plaintiff, unless the court determines there to be a credible reason for not granting the privacy request.

In addition, while the Criminal TAKE IT DOWN Act punishes threatening behavior, neither of the DEFIANCE Act's iterations have provisions that encompass threats, which may leave some survivors without a viable avenue of recourse. This is particularly disheartening because the Senate's findings specifically note that digital forgeries are "often used to . . . commit extortion."[161] Even if the current majority of nonconsensual sexual deepfakes do not target intimate partners or involve threatening behavior, it is important to structure legislation that covers this harmful tool of coercion and control since the rate of intimate partner abuse through deepfakes could exponentially increase at any moment.[162] Senator Durbin's office believes that the legislation captures threatening behavior, as threats to disclose non-consensual intimate imagery are per se evidence of an "intent to disclose."[163] However, not specifically enumerating threatening behavior as an actionable offense can create an unnecessary uphill battle for victims. For example, New York's unlawful dissemination statute, N.Y. Penal Law § 245.15, does not include a provision for threatening behavior, which proved faulty in *People v. Beausejour*.[164] There, Complainant's boyfriend threatened to disseminate an intimate image of complainant if she "continued to refuse [him]," but the case was dismissed for not meeting the intent to cause harm requirement.[165] If a threatening provision were available, this harmful behavior would have been covered. Thus, the Defiance Act should be clear that threatening to release nonconsensual deepfake

161. S. 3696, 118th Cong. § 2(8) (as passed by Senate, July 23, 2024).

162. *See* Lucas, *supra* note 2, at 648 (the percentage of nonconsensual sexual deepfakes targeted at intimate partners is unknown); Telephone Interview with Carrie Goldberg, Attorney, C.A. Goldberg (Oct. 29, 2024) (notes on file with author) (explaining that nonconsensual sexual deepfakes could become a more common problem for survivors of intimate partner violence at any moment and that the entire image-based abuse space is "bracing for impact").

163. *See* Telephone Interview Senate Judiciary Committee Aid (Dec. 3, 2024) (notes on file with author).

164. *See supra* note 41.

165. People v. Beausejour, No. CR-038513-23KN, 2024 NYLJ LEXIS 2303 (N.Y. Crim. Ct. July 18, 2024).

photos is unlawful. Further, a threatening provision that is limited to "threatening the release of nonconsensual sexual deepfakes *with the intent to harass or cause harm*" could allay concerns about broad liability.

Importantly, while civil litigation can be empowering for some survivors, other survivors may prefer a remedy that is less time intensive and costly. Thus, the passage of other types of remedies is critical as well.

VII.
RECOMMENDATIONS FOR LAWMAKERS GOING FORWARD

Given the fervor for combating non-consensual sexual deepfakes, the bipartisan efforts to pass these Bills,[166] and the broad coalitions formed to urge their passage,[167] it is unsurprising that the TAKE IT DOWN Act was passed, and it is entirely possible that the DEFIANCE Act could be passed as well. These Acts and Bills are not perfect, however, they all represent a step in the right direction to combating this problem and providing survivors with multiple options for recourse.

While the TAKE IT DOWN ACT was passed, there are still no federal civil remedies available for survivors. Further, while there is

166. The bipartisan nature of these Bills is continually emphasized by its sponsors. *See, e.g.*, Press Release, Rep. Alexandria Ocasio-Cortez, Rep. Ocasio-Cortez Leads Bipartisan, Bicameral Introduction of DEFIANCE Act to Combat Use of Non-Consensual, Sexually-Explicit "Deepfake" Media (Mar. 7, 2024), https://ocasio-cortez.house.gov/media/press-releases/rep-ocasio-cortez-leads-bipartisan-bicameral-introduction-defiance-act-combat [https://perma.cc/MF5H-8PNH] (Senator Durbin noting that "[w]e've struck a remarkable bipartisan note this Congress [sic] on protecting Americans . . . from exploitation online"); Sen. Cruz's TAKE IT DOWN Act Clears Commerce Committee, *supra* note 104 (defining the TAKE IT DOWN Act as a "[b]ipartisan bill to protect, empower victims of deepfake revenge porn"). Indeed, there is a strong sense that if Congress can get anything done, it should be the passage of deepfake laws. 170 Cong. Rec. S4040 (daily ed. June 12, 2024) (statement of Sen. Richard Durbin) ("There are people who will shake their heads and say: Can't the Senate even address this issue of the sexual exploitation of children and young girls and attempts to ruin their lives? Can't they even agree on a bipartisan basis to come up with an answer? We did.").

167. For example, the TAKE IT DOWN Act has received support from leaders of top technology companies, including Microsoft, Meta, TikTok, and Bumble, a range of victim advocacy groups including RAINN, the largest anti-sexual violence organization in the U.S., and law enforcement. Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Broad Coalition Urges Swift Passage of Sen. Cruz's TAKE IT DOWN Act (Aug. 1, 2024), https://www.commerce.senate.gov/index.php/2024/8/broad-coalition-urges-swift-passage-of-sen-cruz-s-take-it-down-act [https://perma.cc/48RG-RW4J].

an absolute need to pass federal laws to protect survivors, given the ever-changing nature of the federal government, it is also important to ensure that all states have deepfake laws on their books. Thus, this Note concludes by proposing a series of recommendations for future state and federal legislation.

A. All laws should maintain a balance between broad and narrow language to accommodate for evolving technology and ensure that deepfake technology is specifically covered

Criminal and civil laws should define nonconsensual sexual deepfakes with broad language to account for evolving technology. Lawmakers can use the language in the TAKE IT DOWN and DEFIANCE Acts as exemplars for language that accommodates evolving technology.[168] While a statute should be broad, it should also ensure its language will cover nonconsensual sexual deepfakes. For example, the proposed SHIELD Act, a similar criminal bill to the TAKE IT DOWN Act which passed the Senate in 2024 but died at the end of the legislative session, contained such broad language that it risked unintentionally leaving out deepfake content.[169] Lawmakers should adopt similar language to 18 U.S.C § 2256(8),[170] which specifically covers visual depictions that are "created, adapted, or modified to appear that an identifiable [individual] is engaging in sexually explicit conduct" or use language similar to the DEFIANCE or TAKE IT DOWN Acts (digital forgeries that "adapt[], modify[], manipulat[e], or alter[] an authentic visual depiction").[171]

B. Statutes should narrowly tailor liability, but also ensure that proving a statute's elements is not too difficult

Laws must avoid over-inclusivity by requiring a knowledge mens rea or an intent to cause harm when a reckless or negligence mens rea is imposed. At the same time, to ensure this harmful behavior is punished, lawmakers should consider implementing a rebuttable presumption that knowledge that an intimate image is a forgery establishes the subject's lack of consent. While there may be parties

168. *See supra* Parts V.A.1 & B.

169. *See* S. 412, 118th Cong. (2023) (as passed Senate, July 10, 2024) (criminalizing "any visual depiction" but making no mention of if depictions with modifications, adaptions, or any other types of changes fall under the definition).

170. 18 U.S.C. § 2256(8)(C) (2018).

171. *See supra* Parts V.A.1 & B; 47 U.S.C. § 223(h)(1)(B); S. 3696, 118th Cong. § 3(a)(2)(D) (as passed by Senate, July 23, 2024).

that mutually decide to create this content together, a rebuttable presumption ensures that exceptions can be made.

C. All laws should cover threats to release nonconsensual sexual deepfakes

Both criminal and civil laws should explicitly contain provisions on threatening to release deepfake images as this behavior is used to intimidate former partners or strangers and can be deeply damaging. The TAKE IT DOWN Act's provision on threatening behavior serves as a model for other statutes, as it punishes threatening when that person does so "for the purpose of intimidation, coercion, extortion, or to create mental distress."[172] A purpose mens rea ensures that innocuous behavior is covered, while at the same time acknowledging the deep harm of threatening behavior.

D. All civil laws should preserve the privacy of survivors by permitting anonymous filings and allowing for strict discovery requirements

Since a main barrier to filing civil suits is the desire to remain private, civil actions must allow for extensive privacy provisions. This is particularly important given the invasion of privacy that has already occurred through the creation and/or distribution of the nonconsensual sexual deepfake in the first place. While the current privacy protections proposed in the DEFIANCE Act create the option for a court to enact privacy provisions, it does not require a court to do so.[173] Thus, to ensure civil action is utilized, lawmakers should enact a privacy provision that instructs the court to issue privacy protections upon the request of the plaintiff, unless the court determines there to be a credible reason for not granting the plaintiff's privacy wishes.

E. Lawmakers should explore ways to hold platforms accountable

While criminal and civil laws may provide deterrence and address nonconsensual sexual deepfakes after they have been used to abuse another person, they do not fully address the root causes of the problem: the allowance of these deepfakes to be created by applications and proliferate on the internet without platform liability. To comprehensively address this problem, proactive and prospective

172. 47 U.S.C. § 223(h)(6).
173. *See supra* Part VI.C.

tools must be available to prevent the harm from happening in the first place. Going forward, legislators should explore ways to impose liability on platforms that house deepfake creation technology and host the created content. Possible approaches include repealing or creating exceptions to Section 230. This strategy would more holistically combat nonconsensual sexual deepfakes by addressing the underlying creation and proliferation of deepfakes.

VIII.
CONCLUSION

Deepfake technology has emerged as an easily available tool to create realistic photos and videos of an individual doing something they have never done. Nonconsensual sexual deepfakes, the most common type of deepfakes, are a cruel new tool that individuals use to abuse intimate partners and strangers. Survivors of intimate partner violence are particularly vulnerable to nonconsensual sexual deepfakes, since IPV abusers are opportunistic offenders, the technology is widely accessible, and those who have access to more photos/videos of a person can create more realistic deepfakes. While some states have passed laws to combat nonconsensual sexual deepfakes, liability for this behavior greatly varies across jurisdiction and unfortunately, until May 19, 2025, no federal legislation had been passed, largely due to First Amendment and Section 230 restrictions. This note critiques the recently passed TAKE IT DOWN Act and pending DEFIANCE Act and makes suggestions for future legislation. The Acts, while not perfect, are important steps to combatting this abuse. Nonconsensual sexual deepfakes will not disappear anytime soon, and they will continue to evolve with technology. Thus, a holistic approach to combatting this behavior through both civil and criminal federal legislation is imperative going forward.