TAKE IT DOWN TO THE COURTS: COMBATING NONCONSENSUAL INTIMATE DEEPFAKES

Kathryn Z. Mauro[*]

INTRODUCTION 354
I. THE BACKGROUND OF DEEPFAKES 356
II. THE HARMS OF NCII DEEPFAKES 359
III. WAYS TO LEGALLY ADDRESS NCII DEEPFAKE HARMS 362
IV. PLATFORM LIABILITY AND SECTION 230 364
A. Section 230 Reform Efforts 366
B. Section 230 Exceptions 367
V. CREATOR LIABILITY 370
A. State Actions 370
B. Federal Right of Publicity 371
VI. PASSING THE TAKE IT DOWN ACT 374
VII. THREE FEDERAL PATHWAYS 375
A. TAKE IT DOWN Act Section 2 376
B. CPPA & VAWA 378
C. TAKE IT DOWN Act Section 3 381
CONCLUSION 382

[*] J.D. Candidate, Rutgers Law School, May 2026; M.S. Global Affairs, Rutgers University; B.S. Economics, University of Mary Washington. Thank you to my journal note advisor, Professor John R. Kettle, III, my additional sounding board, Professor Cory Poker, and my dear friend, Stephanie I. Robins, for your guidance and feedback on this Note. All errors are my own. Thank you to all the *WRLR* editors. I would also like to thank the Economics and Political Science faculty members at UMW who helped ignite my belief that I could one day get my research published. Thank you to my family, friends, the women of PUP and the Money Squad, and my DTT co-workers for being there for me through this wild part-time law school journey. To my parents, thank you for your unwavering love and support in all my endeavors. Mom, I wish you could have seen this Note's publication.

INTRODUCTION

It's a Monday morning in the United States. The sound of parents calling out to their children to "be in the car to go to school in the next fifteen minutes" rings out from downstairs. In one home, a girl quickly messages her friend a photo of her outfit hoping for some feedback. Instead, in reply, she receives a link. She opens it and her whole body goes numb. She's stunned, flooded with panic, embarrassment, and confusion. She stares at her face on a body that is not hers, in a realistic looking video displaying sexually explicit acts she has never engaged in. There is no way of knowing who made the video or who has seen its contents. A plea to get in the car echoes again from downstairs, but she's frozen. A knock pierces through the shock, and she opens her bedroom door.[1]

In a different town, another knock on a bedroom door reverberates. There is no response, not even a rustling from inside the room. The door opens to make sure their son is awake. His parent expects to see him sleeping and blissfully unaware that they have been calling for him to get to the car. Instead, their eyes land on their child's lifeless body on the floor. They collapse near their son in anguish, unaware of the wail that escapes their body as they call out to their partner to call 9-1-1.[2]

Within the last two years, scenarios like the foregoing have increased in frequency; the people harmed are victims of rapid advancements in deepfake artificial intelligence (AI) technology.[3] It is likely that these events will continue to increase in frequency as AI technology improves. This Note

---

[1] *See* Emily Pascale, Note, *Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse*, 73 SYRACUSE L. REV. 335, 336-37 (2023); Julie Jargon, *Fake Nudes of Real Students Cause an Uproar at a New Jersey High School*, WALL ST. J. (Nov. 2, 2023), https://www.wsj.com/tech/fake-nudes-of-real-students-cause-an-uproar-at-a-new-jersey-high-school-df10f1bb [https://perma.cc/MMQ2-QWT9]; Cyrus Farivar, *Almost Half The Girls At This School Were Targets Of AI Porn. Their Ex-Classmates Have Now Been Indicted.*, FORBES (Dec. 11, 2024), https://www.forbes.com/sites/cyrusfarivar/2024/12/11/almost-half-the-girls-at-this-school-were-targets-of-ai-porn-their-ex-classmates-have-now-been-indicted/ [https://perma.cc/2UVL-2B8T].

[2] *See* Rachel Hale, *These Teenage Boys Were Blackmailed Online and it Cost Them Their Lives*, USA TODAY (Feb. 25, 2025), https://www.usatoday.com/story/life/health-wellness/2025/02/25/teenage-boys-mental-health-suicide-sextortion-scams/78258882007/ [https://perma.cc/D5T4-ABXW] ("The rise of generative artificial intelligence tools has enabled scammers to create highly realistic deepfake images and videos. In some cases, children and teens were blackmailed even when they didn't send a nude image. Roughly 1 of 10 reports Thorn reviewed involved artificially generated content."); *FinCEN Issues Notice on Financially Motivated Sextortion,* FIN. CRIMES ENF'T NETWORK (Sep. 8, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-notice-financially-motivated-sextortion [https://perma.cc/8XBX-GL2T].

[3] *See* Hale, *supra* note 2; FIN. CRIMES ENF'T NETWORK, *supra* note 2; Mariel Padilla, *With AI, Anyone Can Be a Victim of Nonconsensual Porn. Can Laws Keep Up?*, THE 19TH NEWS (Mar. 11, 2024), https://19thnews.org/2024/03/ai-deepfakes-legislation/ [https://perma.cc/CFH9-LTFU]; Kat Tenbarge, *Found Through Google, Bought with Visa and Mastercard: Inside the Deepfake Porn Economy*, NBC NEWS (Mar. 27, 2023, at 11:56 ET), https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071 [https://perma.cc/Q7NS-JBHF].

focuses on Nonconsensual Intimate Imagery (NCII) developed using AI deepfake technology.[4] The use of the term NCII in this Note does not include intimate imagery created consensually or without the use of AI manipulation of the media. This Note narrowly focuses on the nonconsensual use of images of real people, manipulated through AI computer software, to create intimate, sexually explicit, media.

Legislation has lagged behind AI deepfake technology, and while the recently enacted Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act) is a significant achievement, it is not comprehensive enough to address many NCII harms.[5] It remains to be seen whether social media platforms will adhere to one of the TAKE IT DOWN Act's key provisions, the requirement of establishing a removal process for NCII.[6] If there is no removal procedure put in place by May 19, 2026[7], and the Federal Trade Commission does not enforce penalties for failure to adhere, victims may be left without an inexpensive and prompt way to ensure violative media removal from social media platforms.[8] This Note offers actionable recommendations on how to provide victims of NCII with legal recourse under 15 U.S.C. § 6851, 18 U.S.C. §§ 2251-2260A, and the new TAKE IT DOWN Act.

Part One outlines the origins of deepfakes, the technology behind creating deepfakes, and how the evolution of the technology made deepfake creation readily accessible to the average person with little to no programming skills.[9] Part Two highlights the harms faced by victims due to the proliferation of deepfakes. Including concerns that the proliferation of

---

[4] Trudi K. Sundberg, Note, *Federalizing NCII Regulation: The Take It Down Act's Approach to Criminalization, Platform Liability, and Threats to Disseminate*, 59 GA. L. REV. 1207, 1210-11 (2025) ("NCII abuse refers to image-based sexual abuse or nonconsensual pornography. . . Nonconsensually produced intimate images can either be produced without the victim's knowledge or self-generated by grooming or pressuring a victim into production.").

[5] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, Pub. L. No. 119-12, 139 Stat. 55 (2025) (codified as amended at 47 U.S.C. §§ 223–223a).

[6] *Id.*

[7] 47 U.S.C. § 223a(a)(1)(A).

[8] *Cruz-Klobuchar Bill to Protect Teenagers from Deepfake 'Revenge Porn' Unanimously Passes the Senate*, U.S. SENATE COMM. ON COM., SCI., & TRANSP.: PRESS RELEASES (Feb. 13, 2025) [hereinafter *Cruz-Klobuchar Bill to Protect Teenagers*], https://www.commerce.senate.gov/index.php/2025/2/cruz-klobuchar-bill-to-protect-teenagers-from-deepfake-revenge-porn-unanimously-passes-the-senate [https://perma.cc/4AN9-U9S6] ("[V]ictims struggle to have images depicting them removed from websites, increasing the likelihood the images are continuously spread, and victims are traumatized. In 2022, Congress passed legislation creating a civil cause of action for victims to sue individuals responsible for publishing NCII. However, bringing a civil action can be incredibly impractical. It is time-consuming, expensive, and may force victims to relive trauma."); Pei-Sze Cheng & Jennifer Millman, *Long Island Man Jailed in Deepfake Sex Scheme Targeting 11 Women From His High School*, NBC N.Y., 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/T4EZ-YD7Z] (last updated Apr. 19, 2023).

[9] Jargon, *supra* note 1.

deepfakes will harm the public's general trust of all videos and erode, what scholars call, the epistemic backstop of video evidence.[10]

Part Three gives an overview of ways to legally address the harms posed by the distribution and creation of NCII deepfakes. Part Four describes the historic complications of holding information content providers, such as social media platforms, liable because of Section 230 of the Communications Decency Act. Part Five discusses the difficulties of creator and distributor liability for NCII. Part Six provides a brief discussion of the TAKE IT DOWN Act's path to becoming law.

Lastly, Part Seven offers three federal pathways to help victims reclaim their image and address the harms associated with the creation and distribution of NCII. This Note argues that the TAKE IT DOWN Act provides important, yet incomplete, federal legal recourse for victims of NCII. The first pathway for recourse is through the government filing criminal charges under Section 2 of the TAKE IT DOWN Act. The second pathway is for victims to use the private right of action under federal laws governing the disclosure of intimate images under the 2022 Reauthorization of the Violence Against Women Act (VAWA)[11] and the prevention of the sexual exploitation of children under the Child Pornography Prevention Act of 1996 (CPPA).[12] The third pathway is for victims to utilize Section 3 of the TAKE IT DOWN Act to request removal of NCII from covered platforms. Pursuing this third pathway will also determine whether the TAKE IT DOWN Act will pass constitutional muster given current court interpretations of Section 230.

I. THE BACKGROUND OF DEEPFAKES

The concerns surrounding nonconsensual computer-generated images, also known as deepfakes, have increased across various disciplines and within the legal field.[13] Deepfakes derive their name from "a portmanteau of

[10] *E.g.*, Regina Rini, *Deepfakes and the Epistemic Backstop*, 20 PHILOSOPHERS' IMPRINT 1, 7 (2020); Taylor Matthews & Ian James Kidd, *The Ethics and Epistemology of Deepfakes*, *in* THE ROUTLEDGE HANDBOOK OF PHIL. AND MEDIA ETHICS, 342, 351 (Carl Fox & Joe Saunders eds., 2023); Don Fallis, *The Epistemic Threat of Deepfakes*, 34 PHIL. & TECH. 623, 627 (2021); Catherine Kerner & Mathias Risse, *Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds*, 8 MORAL PHIL. AND POL. 81, 98 (2020).

[11] 15 U.S.C. § 6851.

[12] 18 U.S.C. §§ 2251-2260A.

[13] *See, e.g.*, Michelle M. Grahm, *Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat*, THOMSON REUTERS (June 26, 2024), https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/ [https://perma.cc/4XZR-TZCZ] (discussing ten states that enacted deepfake regulations and four states that have regulations pending in areas spanning election campaign communications to deepfakes of minors engaging in sexual conduct); Sara Asher, Comment, *A Federal Right of Publicity to Navigate The Wild West of Generative AI Content*, 36 ST. THOMAS L. REV. 105, 117 (2024); Niki Saenz, Note, *Let's Be Realistic: Crafting an Effective Legal*

deep learning and fake."[14] Legal academics have defined deepfakes as the creation of fabricated, yet realistic, audiovisual material of actual people engaged in behavior that never took place utilizing AI machine learning (ML) algorithms.[15] The Merriam-Webster Dictionary defines a deepfake as "an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said."[16] Although it appears as a new phenomenon, this problem with AI ML deepfakes initially caused concern in 2017.[17]

The first media publication about deepfakes appeared in a *Motherboard* article, in December 2017, reporting on a Reddit user by the name of "deepfakes."[18] The user created fake pornographic clips of celebrities using open-source AI deep learning software.[19] These early deepfakes created by the Reddit user were noticeably doctored because at certain points celebrity faces did not sync properly with the underlying video.[20] Nevertheless, fellow Reddit users followed suit and Reddit communities devoted to the sharing, creation, and support of developing deepfakes grew to house a wide variety of deepfake material.[21] In the past, deepfakes were harder to make convincing and required access to technology beyond what is necessary today, a smartphone and the right app, instead of advanced computer hardware and software.[22]

The sophistication of deepfakes has grown substantially. Nomenclature has developed to distinguish between falsified images and videos created with and without the use of ML technology. The type of AI ML deep learning involved in creating a deepfake developed from the use of neural networks.[23]

Remedy for Victims of Deepfake Pornography, 66 ARIZ. L. REV. 785, 795 (2024); Rena Song, Note, *Faking It: A Proposed Solution to Counter Nonconsensual Pornographic Deepfakes*, 31 WASH. & LEE J. CIV. RTS. & SOC. JUST. 157, 201-20 (2025).

[14] Matthews & Kidd, *supra* note 10, at 342.

[15] Adrienne de Ruiter, *The Distinct Wrong of Deepfakes*, 34 PHIL. & TECH. 1311, 1312 (2021); Mary Anne Franks & Ari Ezra Waldman, *Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions*, 78 MD. L. REV. 892, 893 (2019).

[16] *Deepfake*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/deepfake [https://perma.cc/DYX2-PTVN] (last visited Dec. 5, 2024).

[17] Samantha Cole, *AI-Assisted Fake Porn is Here and We're All F****d*, VICE, (Dec. 11, 2017), https://www.vice.com/en/article/gydydm/gal-gadot-fake-ai-porn [https://perma.cc/TV2H-XVH2]; Elizabeth A. Safaryn, Note, *The Deepfake Dilemma: Fake Images, Real Victims, and the Legal Void in Addressing Non-Consensual Deepfake Pornography*, 32 WM. & MARY J. RACE, GENDER, & SOC. JUST. 281, 282 (2026).

[18] Cole, *supra* note 17.

[19] *Id.*

[20] *Id.*

[21] Kerner & Risse, *supra* note 10, at 84.

[22] Jargon, *supra* note 1.

[23] Matthews & Kidd, *supra* note 10, at 342.

> Neural networks are a subset of machine learning algorithms with structures that imitate the neurons inside the human brain. They are composed of multiple node layers, including an input layer, hidden layers, and an output layer. . . . Together, these layers form a machine learning model that learns and improves accuracy based on training data.[24]

The type of neural network most frequently used in the creation of deepfakes are generative adversarial networks (GANs) which "mimic[] the way in which learning takes place in the human brain."[25]

GANs utilize two types of algorithms, the generator and the discriminator, to develop and improve upon the quality and realism of the deepfake.[26] The generator portion of the process is conducted by feeding large amounts of material of the desired individual(s) into the program to allow multiple reference points for the algorithm to draw from and learn how to mimic the audiovisual traits of the individual(s).[27] Then, the discriminator evaluates the accuracy and validity of the generated material by comparing the generated material with actual footage fed into the program.[28] The iterative process of analyzing actual material, developing deepfake material, and scrutinizing the developed material creates a feedback loop to continually improve the produced deepfakes.[29]

Scholars describe four distinct ways to create deep-learning alterations:

> First, synthesizing photographs and video input to generate entirely non-existent faces (**entire-face synthesis**). Second, manipulating particular facial attributes that might be characteristic of certain people, which ranges from adding or removing features such as moles and wrinkles to more extensive changes like adjusting the skin color of a person's face (**attribute manipulation**). Third, deep-learning can also swap or replace the facial expressions of one person with those of another, like smiles, snarls, grimaces, looks of confusion or disgust and so on (**expression swap**). Fourth, deep-learning techniques can replace the identity of one person and swap it with another (**identity swap**).[30]

NCII creation generally falls within the "identity swap" category.

Nomenclature has developed to distinguish between falsified images and videos created with and without the use of ML technology. "Cheapfakes,"[31] occasionally referred to as shallow fakes, are defined as manipulated videos

---

[24] Kate Kobriger et al., Note, *Out of Our Depth with Deep Fakes: How the Law Fails Victims of Deep Fake Nonconsensual Pornography*, 28 RICH. J.L. & TECH. 204, 210-11 (2021).

[25] de Ruiter, *supra* note 15, at 1314.

[26] *Id.* at 1314-15; Matthews & Kidd, *supra* note 10, at 342-43.

[27] de Ruiter, *supra* note 15, at 1314-15.

[28] *Id.*

[29] *Id.*

[30] Matthews & Kidd, *supra* note 10, at 343 (emphasis added).

[31] de Ruiter, *supra* note 15, at 1315.

or images without the use of deep learning AI technology, often developed via commercial software such as Adobe Inc.'s Photoshop®, slowing down, or speeding up videos, or otherwise manipulating the audiovisual representation of the people in the original content.[32] Conversely, deepfakes are manipulated videos or images developed using AI ML technology.[33] The increase in ease of creation and realism of deepfakes creates legally cognizable harms that must be addressed before the technology and dissemination of deepfakes further outpaces the legal system.

II. THE HARMS OF NCII DEEPFAKES

The first widespread development of deepfakes was the creation of female celebrity deepfake pornography for entertainment purposes using readily available images of famous women to create the deepfake.[34] "According to Sensity, an Amsterdam-based company that detects and monitors AI-developed synthetic media for industries like banking and fintech, 96 percent of deepfakes are sexually explicit and feature women who didn't consent to the creation of the content."[35] The proliferation of NCII has concerned governments and led many to begin to seek ways to combat the harms.

In October of 2022, the United States Department of Homeland Security noted in the *Increasing Threat of Deepfake Identities* report that researchers determined "more than 100,000 computer-generated fake nude images of women [have been] created without their consent or knowledge."[36] On October 30, 2023, former President Biden issued an executive order with a charge to solve the problem of "generative AI . . . producing nonconsensual intimate imagery of real people."[37] Most recently, on May 19, 2025, the bipartisan TAKE IT DOWN Act was signed into law.[38]

This type of federal action is all the more important due to the increase in the ease of creating deepfakes and the almost ubiquitous access to

---

[32] *Id.*; Matthews & Kidd, *supra* note 10, at 342.

[33] Matthews & Kidd, *supra* note 10, at 342.

[34] Cole, *supra* note 17; Safaryn, *supra* note 17, at 282.

[35] Tenbarge, *supra* note 3; *see* Safaryn, *supra* note 17, at 284 ("Of the 14,678 deepfake videos circulating on the Internet in 2019, 96 percent were pornographic deepfakes.").

[36] U.S. DEP'T OF HOMELAND SEC., INCREASING THREAT OF DEEPFAKE IDENTITIES (2021); No Artificial Intelligence Fake Replicas And Unauthorized Duplications Act of 2024, H.R. 6943, 118th Cong. (2024) (as referred to the H. Comm. on the Judiciary, Jan. 10, 2024).

[37] Frank Figliuzzi, *A loophole makes it hard to punish these despicable AI-generated nude photos*, MSNBC (Nov. 7, 2023, at 20:26 ET), https://www.msnbc.com/opinion/msnbc-opinion/ai-generated-nudes-new-jersey-students-rcna123931 [https://perma.cc/HG9B-XN9C].

[38] 47 U.S.C. §§ 223–223a; Press Release, Amy Klobuchar Minnesota, Klobuchar's Bipartisan TAKE IT DOWN Act Signed into Law (May 19, 2025) [hereinafter TAKE IT DOWN Act Signed into Law], https://www.klobuchar.senate.gov/public/index.cfm/2025/5/klobuchar-s-bipartisan-take-it-down-act-signed-into-law [https://perma.cc/4AN9-U9S6].

smartphones among children, increasing the possibility of the average individual becoming a victim of NCII. In the fall of 2023, a group of high school girls in Westfield, NJ were victims of AI generated nude images created by their male classmates.[39] Around the same time, two teenage boys in Lancaster, PA created over 300 deepfake pornographic images using the public social media accounts of sixty different girls, including forty-eight of their female classmates.[40]

There is an alarming concern with deepfakes, particularly those of a pornographic nature, that deletion can never truly occur.[41] Nonconsensual deepfake violations are so destructive because our self-image and conception of our identity are so deeply connected to our voice and face.[42] Deepfakes remove our rights to our digital self-representation.[43] Deepfake creators and requestors acknowledge that a deepfake does not need to be believable or believed to be effective if your aim is reputational harm.[44] When distribution occurs and the information presented is false, the false information often overrides accurate information.[45]

Reputational harm is not the only potential injury realized by NCII victims. Victims face threats to their physical, mental, and financial wellbeing.[46]

> A 2017 study of more than 3,000 victims of [nonconsensual pornography (NCP)] observed increased somatic symptoms and decreased mental health inventory in victims. Victims of NCP report offline, in-person conduct that threatens their physical wellbeing, such as harassment and stalking as a result of the NCP. The experience almost universally tolls their mental health, with a staggering [fifty-one percent] of victims reporting suicidal thoughts and [ninety-three percent] reporting significant emotional distress resulting from the NCP. The mental health effects are similar to those experienced by rape survivors. NCP also impacts victims' financial wellness by impairing their occupational functioning, which can force them to take time off work or school, cause them to drop out of school, or even result in termination from employment. More than half of victims fear that the NCP will affect their professional advancement even decades into the future.[47]

---

[39] Jargon, *supra* note 1.

[40] Farivar, *supra* note 1.

[41] Jesselyn Cook, *Here's What It's Like to See Yourself in a Deepfake Porn Video*, HUFFPOST (June 23, 2019), https://www.huffpost.com/entry/deepfake-porn-heres-what-its-like-to-see-yourself_n_5d0d0faee4b0a3941861fced [https://perma.cc/BFP4-L293].

[42] de Ruiter, *supra* note 15, at 1313-14.

[43] *Id.* at 1327-28.

[44] Rini, *supra* note 10, at 6.

[45] Franks & Waldman, *supra* note 15, at 895.

[46] Kobriger et al., *supra* note 24, at 209.

[47] *Id.* at 209-210.

These concerns and injuries are important public policy considerations when developing laws to hold creators and distributors accountable. The variety of tangible harms faced by victims illustrates why uniform federal redress is so important.

Even though the overwhelming majority of deepfakes produced are pornographic in nature, it is important to acknowledge the other areas impacted by the creation of deepfakes. Deepfakes emerged in the political discourse, as early as the leadup to the 2020 United States Presidential election.[48] This threat initiated proposed solutions for how to spot deepfakes and prevent their proliferation across platforms to address concerns of potential United States election disruption.[49] Conducting election manipulation by way of deepfakes may occur

> through 'crowd-turfing' – a technique used in the fields of campaigning and marketing to manufacture the appearance (or absence) of popular support . . . [or] it may soon be possible to tweak (in real time) a live feed of facial expressions of those filmed listening to a candidate speaking . . . [eroding] the unconscious cues we use

as mechanisms of determining emotions, impressions, and support.[50]

However, subjecting individuals to harm through negative uses of deepfake technology is not the only outcome of the increased ease in developing deepfakes. Use of deepfake technology in entertainment has allowed for the creation of interactive experiences that may prove educational and increase interest in museums.[51] Additionally, the use of deepfake technology protected the identities of LGBTQ+ "individuals who suffered from persecution in Russia [and] were able to testify of their experiences in [a] documentary *Welcome to Chechnya*."[52]

Nevertheless, a concern of many scholars is that the continued and increased proliferation of deepfakes in society will lead to a decline in the trustworthiness of information obtained through videos and that this decline will lead to a general distrust of all videos.[53] This stands, not only to place the use of audio or video evidence in the legal system in jeopardy in general, but to increase the difficulty in holding those that target individuals through

---

[48] David Ingram & Jacob Ward, *How do you spot a deepfake? A Clue Hides Within Our Voices, Researchers Say*, NBC NEWS (Dec. 16, 2019), https://www.nbcnews.com/tech/tech-news/little-tells-why-battle-against-deepfakes-2020-may-rely-verbal-n1102881 [https://perma.cc/NH89-6ZTR].

[49] *Id.*

[50] de Ruiter, *supra* note 15, at 1318 (internal quotations omitted) (citation omitted).

[51] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1769 (2019).

[52] de Ruiter, *supra* note 15, at 1316.

[53] *E.g.*, Rini, *supra* note 10, at 7; Matthews & Kidd, *supra* note 10, at 345; Fallis, *supra* note 10, at 625; Kerner & Risse, *supra* note 10, at 98.

deepfakes responsible for their actions.[54] The slow pace at which the legal system has responded to the distribution of harmful deepfakes has forced victims to rely on overwhelmingly paltry policies implemented by individual companies to attempt to remediate the harm to victims and seek the removal of deepfake pornography.[55]

Popular social media corporations, including Reddit, Meta, and X, have responded to deepfakes by modifying some of their policies.[56] For example, "Reddit banned the deepfake community for violating its 'involuntary pornography' rules" after widespread media reporting.[57] Individuals can request that Google remove pages from their search that include "involuntary fake pornography."[58] Discord relies on community guidelines that "prohibit the coordination, participation or encouragement of sexual harassment," and have removed servers or platforms selling the creation of deepfakes for violations of "content or behavior that sexualizes or sexually degrades others without their apparent consent."[59] Even adult entertainment websites have provisions against deepfake content.[60] However, actions by individual corporations will continue to be an insufficient attempt to redress the harms until it is determined that the legal system is able to provide a more widespread federal solution through the prosecution of those that create and distribute NCII.

III. WAYS TO LEGALLY ADDRESS NCII DEEPFAKE HARMS

There are two ways to provide legal recourse for the harms caused by the distribution and creation of deepfakes. First, laws can hold platforms and applications where the distribution takes place accountable.[61] Second, laws can hold creators and distributors accountable through criminalizing the activity and/or providing individuals harmed with a private right of action to

---

[54] Rini, *supra* note 10, at 8.

[55] Song, *supra* note 13, at 189-95.

[56] Kerner & Risse, *supra* note 10, at 105; *see* Song, *supra* note 13, at 189-95.

[57] Rini, *supra* note 10, at 5.

[58] Tenbarge, *supra* note 3.

[59] *Id.*

[60] Some adult entertainment websites have provisions under their non-consensual content policy guidelines that include the following language: "To help protect the integrity of the platform, we also prohibit content, including fictional, simulated, or animated, that features or depicts: . . . Any 'deepfakes' whatsoever (AI-generated, modified, or other manipulations of a person's image, whether in picture or video, to deceive or mislead the viewer into believing that person is acting or speaking in the way presented)." *Non-Consensual Content Policy*, PORNHUB (Sep. 2025), https://help.pornhub.com/hc/en-us/articles/4419871787027-Non-Consensual-Content-Policy [https://perma.cc/HK63-EE78]; *Non-Consensual Content Policy*, REDTUBE (Oct. 2024), https://www.redtube.com/non-consensual-content-policy [https://perma.cc/5E86-KU8W].

[61] *See* Kavyasri Nagumotu, Note, *Deepfakes are Taking Over Social Media: Can the Law Keep Up?*, 62 (2) IDEA 102, 128-31 (2022); Saenz, *supra* note 13, at 792-99.

civilly sue the creators and distributors.[62] However, there are challenges to each path in providing a remedy. While "the consensus is that we need a global, collaborative response to these issues," it is likely a long way off and therefore, the best course of action in the United States is to continue to enact federal legislation, like the TAKE IT DOWN Act, to hold platforms, creators, or both liable.[63]

Arguably, holding social media platforms accountable[64] may be one of the most impactful ways to provide legal recourse to victims of NCII deepfakes.[65] This angle of attack removes the concern of finding the original creator of the deepfake, which is often close to impossible depending on the sophistication and knowledge of the creator.[66] Focusing on finding a way to hold platforms accountable also removes the concern of jurisdictional access to creators outside of the United States.[67] Social media platforms are entities within reach of the United States jurisdiction and cannot go undetected like individual creators.

Globally, nations have taken a variety of approaches to address the problem of deepfakes.[68] Nations like China and Australia are attempting to combat deepfakes through federal law enforcement and regulations.[69] "The Chinese government has . . . enacted strict regulations, called Deep Synthesis Provisions, which prohibit the creation of deepfakes without the consent of the user and require confirmation that the content was generated using AI."[70] The United Kingdom passed amendments to their Online Safety Bill to ban nonconsensual deepfake pornography.[71] Denmark introduced a bill to

---

[62] This Note treats creator and distributor as one and the same because generally, the individual that created the nonconsensual deepfake pornography also shares it through one or multiple messaging applications or social platforms. *See* Isabella Constantino, Comment, *Real People in Fake Porn: How a Federal Right of Publicity Could Assist in the Regulation of Deepfake Pornography*, 64 JURIMETRICS J. 263, 277-84 (2024); Saenz, *supra* note 13, at 810-13.

[63] Tenbarge, *supra* note 3.

[64] Section 3 of the TAKE IT DOWN Act requires the Federal Trade Commission to enforce covered platforms providing a notice and removal process for intimate visual depictions. 47 U.S.C. § 223a(b).

[65] *See* Kobriger et al., *supra* note 24, at 253.

[66] Nagumotu, *supra* note 61, at 125-26.

[67] Chesney & Citron, *supra* note 51, at 1792.

[68] *See, e.g.*, Amelia Nierenberg, *Denmark Aims to Use Copyright Law to Protect People From Deepfakes*, THE NEW YORK TIMES (July 10, 2025), https://www.nytimes.com/2025/07/10/world/europe/denmark-deepfake-copyright-ai-law.html [https://perma.cc/PQ65-A4E8]; Caroline Quirk, *The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology*, PRINCETON LEGAL J. (June 19, 2023), https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/ [https://perma.cc/3SFN-VVRR]; Tenbarge, *supra* note 3.

[69] Jordanna Schriever, *Deepfakes Back in the Headlines After a Federal Law Was Used for the First Time*, ABC AUSTL. (Feb. 26, 2026), https://www.abc.net.au/news/2026-02-27/rise-in-sexualised-deepfakes-new-laws-explainer/106390940 [https://perma.cc/94LQ-PLB4]; Quirk, *supra* note 68.

[70] Quirk, *supra* note 68.

[71] *Id.*

expand their copyright laws to include rights over each individual's own likeness.[72] However, until the TAKE IT DOWN Act, the United States struggled to pass legislation placing any form of liability on platforms because of Section 230 of the Communications Decency Act.[73]

IV. PLATFORM LIABILITY AND SECTION 230

In the United States, attempts to hold platforms accountable for the torts of their users have largely failed due to protections under Section 230 of the Communications Decency Act, the only section of the Act not struck down by the Supreme Court for First Amendment violations.[74] Subsection 230(c)(1) stipulates that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[75] Courts have generally given platforms that fall under the definition of an interactive computer service expansive freedom under Section 230.[76] Yet, "[j]udges have denied Section 230(c)(1) protection in two situations: (1) where the platform, at least partly, developed or created the content; and (2) where the claim did not treat the platform as the publisher or speaker of third-party content."[77]

Prior to the enactment of Section 230, courts primarily treated platforms as distributors with very limited liability, similar to bookstores and newsstands, instead of as publishers, with responsibility for the work of their authors (both employed and freelance).[78] *Cubby, Inc. v. CompuServe* was the first case where a judge applied the standards of distributor liability to an online forum.[79] The court found in favor of CompuServe because, although CompuServe could decline to carry certain third-party content, once they allowed publication, they had "little to no editorial control over that publication's contents."[80] The court found CompuServe to be a distributor and Cubby failed to demonstrate that CompuServe "knew or had reason to

---

[72] Nierenberg, *supra* note 68.

[73] 47 U.S.C. § 230(c).

[74] *See, e.g.*, Mary Anne Franks, *How the Internet Unmakes Law*, 16 OHIO ST. TECH. L.J. 10, 11-12 (2020); Sundberg, *supra* note 4, at 1218.

[75] 47 U.S.C. § 230(c)(1).

[76] *See* Jeff Kosseff, *A User's Guide to Section 230, and A Legislator's Guide to Amending it (or Not)*, 37 BERKELEY TECH. L.J. 757, 773-79 (2022) (discussing how the broad interpretation of § 230(c)(1) came to be).

[77] *Id.* at 779-80.

[78] *See* Nagumotu, *supra* note 61, at 129; Kosseff, *supra* note 76, at 761-68.

[79] Kosseff, *supra* note 76, at 765-66; *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (granting summary judgement for defendant database because plaintiffs failed to show genuine issue of material fact on whether defendant knew or had reason to know of the alleged libelous statements).

[80] *Cubby*, 776 F. Supp. at 140; Kosseff, *supra* note 76, at 765-66.

know" the substance of the forum's materials.[81] In most jurisdictions, the only guidance courts could find to help address issues of platform liability were non-binding decisions.[82] Courts upheld the standard set by *Cubby, Inc.* determining "that platforms [receive] greater liability protection if they [take] a hands-off approach to user content."[83] This treatment of platforms by the courts informed the creation of Section 230.[84]

After the passage of Section 230, courts broadened platform protection by interpreting a distributor to be a type of publisher which shields platforms from liability even if they "knew or had reason to know of defamatory user content."[85] This interpretation of Section 230(c)(1) prohibits "any claim against an interactive computer service provider arising from third-party content unless an exception applied."[86] The first federal case to interpret Section 230(c)(1) was decided in 1997, *Zeran v. America Online*, when the 4th Circuit affirmed a district court ruling and settled on the broad interpretation that set the standard adopted by judges.[87] Section 230 "has gone largely unchallenged by judges over the past [more than a] quarter century."[88] Moreover, it is still undetermined whether the Supreme Court would follow this interpretation.[89]

Although the overwhelming majority of Section 230 decisions involve Section 230(c)(1), the subsequent portion of the act, Section 230(c)(2), provides additional liability protections for platforms that are involved in "develop[ing], even in part, the content at issue."[90] Consequently, "platforms enjoy immunity from liability for user-generated content even if they deliberately encouraged the posting of that content."[91] Immunity from liability is also afforded to platforms that participate in the moderation of postings through a good-faith effort to delete objectionable content.[92]

---

[81] *Cubby*, 776 F. Supp. at 141; Kosseff, *supra* note 76, at 766.

[82] Kosseff, *supra* note 76, at 768 ("In 1995, *Cubby* and *Stratton Oakmont* were the only U.S. court opinions that examined the liability of online services for the user content they distributed. Although these rulings were not binding on other courts, they were the only opinions that other judges could look to for guidance. And they suggested that platforms received greater liability protection if they took a hands-off approach to user content.").

[83] *Id.* at 768.

[84] *See* Nagumotu, *supra* note 61, at 128-29; Kosseff, *supra* note 76, at 770.

[85] Kosseff, *supra* note 76, at 774.

[86] *Id.*

[87] *Id.* at 774-76; *see generally* Zeran v. America Online, 958 F. Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997) (holding Section 230 grants broad federal immunity for service providers under publisher and distributer liability).

[88] Kosseff, *supra* note 76, at 785.

[89] *Id.* at 785 ("The Supreme Court has never interpreted the scope of Section 230."); *see* Saenz, *supra* note 13, at 793.

[90] Barnes v. Yahoo! Inc., 570 F.3d 1096, 1105 (9th Cir. 2009) (internal citations omitted); Kosseff, *supra* note 76, at 779.

[91] Chesney & Citron, *supra* note 51, at 1796.

[92] Kosseff, *supra* note 76, at 779.

However, there have been calls for changes to the interpretation of, or modification to, Section 230 from judges and Congressional representatives.[93]

A. Section 230 Reform Efforts

Congress has introduced various types of proposed legislation over the past six years to address concerns about Section 230.[94] The bills fall into four types of reform categories:

> **Repeal:** Bills that repeal Section 230 in whole. **Limiting the Scope:** Bills that restrict the types of activities protected by Section 230. These bills would prohibit companies from using Section 230 as a defense under certain conditions, such as in cases of child sexual exploitation or civil rights violations. **Imposing New Obligations:** Bills that impose new obligations (such as a duty of care or quid pro quo requirements) on companies that wish to use Section 230 as a defense. **Good Samaritan:** Bills that alter the "Good Samaritan" portion of Section 230. This includes bills that attempt to address perceived political bias or censorship.[95]

However, within the last six years, only two of the over fifty bills introduced have passed, the TAKE IT DOWN Act and the Daniel Anderl Judicial Security and Privacy Act, enacted as part of the 2023 National Defense Authorization Act (NDAA).[96]

The Daniel Anderl Act, provided as "Subtitle D – Judicial Security and Privacy," of the 2023 NDAA,[97] falls under the "Imposing New Obligations" category outlined above. The Daniel Anderl Act requires "any person, business, or association, once notified," to remove "covered personal information of federal judges or their family members."[98] The application of the law was also retroactive and required businesses to comply with the change within seventy-two hours of a formal request notification.[99]

The Daniel Anderl Act introduced platforms and tech companies to novel potential liabilities.[100] Under the Act, tech companies must "implement and maintain reasonable security procedures to ensure their compliance with

---

[93] *Id.* at 785-88.

[94] Meghan Anand et al., *All the Ways Congress Wants to Change Section 230*, SLATE, https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html [https://perma.cc/E88W-MCPD] (last updated Sep. 19, 2023).

[95] *Id.* (emphasis added).

[96] *See id.*; *e.g.*, 47 U.S.C. §§ 223–223a; James M. Inhofe National Defense Authorization Act, 138 U.S.C. §§ 117-263 (2022).

[97] 138 U.S.C. §§ 117-263 § 5931.

[98] Anand et al., *supra* note 94.

[99] *Id.*

[100] *Id.*

provisions."[101] Failure to comply with the removal of covered information opens up platforms and tech companies to liabilities "for an amount equal to actual damages sustained by judges and their families and for the plaintiff's legal fees."[102]

While the final version of this law does not directly mention Section 230, a previous version overtly mentioned Section 230 and specified that "[n]othing in this subtitle shall be construed . . . to impose liability on an interactive computer service in a manner that is inconsistent with the provisions of section 230, but only if the service complies with a request to remove content under the amendment."[103] In other words, so long as the service complied with the removal of the content regarding the judge or their families, Section 230 maintains protection against liability. The final version of the Daniel Anderl Act omitted this reference to Section 230, thus implying that courts may impose liabilities on platforms under this law that Section 230 would otherwise prohibit.

Similarly, Section 3 of the TAKE IT DOWN Act, requiring a notice and removal process for nonconsensual intimate visual depictions from covered platforms, does not explicitly mention Section 230.[104] Section 3 requires covered platforms to remove the image, and reasonably attempt to remove any identical copies, no more than forty-eight hours after receipt of a valid removal request.[105] Covered platforms may qualify for a limitation on liability where there has been a "good faith" effort of image removal.[106] However, it remains to be seen what courts identify as "good faith" under the TAKE IT DOWN Act and whether they interpret Section 3 to be at odds with Section 230.

B. Section 230 Exceptions

Proposed solutions to provide recourse to victims of NCII have primarily focused on the immunity exceptions present in Section 230(e).[107] 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.[108] Most proposals fall under one of the first three exceptions.[109]

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] 47 U.S.C. § 233a.
[105] *Id.*
[106] *Id.*
[107] 47 U.S.C. § 230(e); *see* Saenz, *supra* note 13, at 793-810.
[108] 47 U.S.C. § 230(e).
[109] *See* Saenz, *supra* note 13, at 793.

State laws are the most prevalent response to the increasing incidents of nonconsensual deepfake pornography.[110] Section 230(e)(3) allows states to enforce "any state law that is consistent with this section."[111] However, 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."[112] Although Congress did not provide a definition of what it means for a state law to be "consistent with" Section 230, courts primarily determine this based on whether Section 230(c)(1) is violated by the state law's treatment of the platform as a publisher.[113] Therefore, state laws overwhelmingly focus on creator liability instead of platform liability in an attempt to avoid Section 230 violations.[114]

Looking beyond the state level, most of the recent proposed legislation and academic recommendations fall under Section 230(e)(2), which states, "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property."[115] Victims can attempt to pursue copyright infringement claims against "the deepfake creator and the platform circulating such content."[116] However, victims may not be able to overcome the challenges of proving they are the owner of the copyright or successfully combating a fair use defense.[117] Consequently, these recommendations tend to focus on establishing a federal right of publicity.[118] Generally, the difficulty in avoiding Section 230 immunity lies in the fact that there is no definition of "intellectual property" and "circuits interpret the term differently."[119] Therefore, similarly to state actions, these proposals primarily provide an avenue for creator liability and not platform liability.[120]

Some argue for the establishment of federal criminal legislation.[121] Section 230(e)(1) provides that any defendant in a federal criminal prosecution cannot claim immunity under Section 230.[122] Although one of the best ways to prevent the harms of NCII may be to hold platforms liable,

---

[110] *Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Nov. 22, 2024), https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation (on file with the WRLR).

[111] 47 U.S.C. § 230(e)(3).

[112] Saenz, *supra* note 13, at 794.

[113] *Id.* at 795.

[114] NAT'L CONF. OF STATE LEGISLATURES, *supra* note 110.

[115] 47 U.S.C. § 230(e)(2).

[116] Safaryn, *supra* note 17, at 289.

[117] *Id.* at 289-90 (explaining the challenges involved in victims bringing copyright infringement claims against the creators of deepfakes and online platforms).

[118] *E.g.*, H.R. 6943; Asher, *supra* note 13, at 109; W. Woods Drinkwater, Note, *Personality Beyond Borders: The Case For A Federal Right of Publicity*, 3 MISS. SPORTS L. REV. 115, 116 (2021).

[119] Saenz, *supra* note 13, at 794 (discussing the variability in how the Ninth Circuit and Third Circuit differ in their interpretations of whether "any law" in Section 230(e)(2) includes protections for established federal intellectual property rights only or also encompasses state intellectual property rights).

[120] *E.g.*, H.R. 6943; Asher, *supra* note 13, at 109; Drinkwater, *supra* note 118.

[121] Saenz, *supra* note 13, at 810-13.

[122] 47 U.S.C. § 230(e)(1).

there are no examples yet of successful federal criminal prosecutions of platforms even when Congress has passed legislation that extends platform liability.[123]

The Allow States and Victims to Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act (FOSTA-SESTA) falls within Section 230 exceptions under (e)(1) and (e)(5). FOSTA-SESTA passed in 2018 and holds platforms and websites liable for supporting and aiding sex trafficking.[124] FOSTA-SESTA creates an exception to Section 230 that makes "websites legally liable for any content that helped facilitate sex trafficking or prostitution."[125] The passage of FOSTA-SESTA initially successfully contributed to multiple platforms shutting down or limiting the type of sexual content posted.[126] Unfortunately, the impact of FOSTA-SESTA has not been very long lasting. Sex trafficking ads still appear on websites and social platforms, and some advocacy groups report an increase in the number of missing and dead sex workers throughout the United States.[127] Despite the inconsistent desired outcomes of FOSTA-SESTA, federal criminal law is still a worthwhile consideration to remedy NCII.

Federal criminal law implementation proposals suggest looking at how the Cyber Civil Rights Initiative (CCRI) suggestions shaped some state nonconsensual pornography laws.[128] These recommendations seek to provide, "(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."[129] This Note suggests that some of these components are present in the TAKE IT DOWN Act, and some components are satisfied through the application of 15 U.S.C. § 6851 and 18 U.S.C. §§ 2251-2260A.[130] Considering the difficulties faced by attempts to increase the liability of interactive computer service providers, any modification to the interpretation of Section 230 will be an uphill battle.

---

[123] Saenz, *supra* note 13, at 809-10.

[124] Liz Tung, *FOSTA-SESTA was supposed to thwart sex trafficking. Instead, it's sparked a movement*, THE PULSE WHYY PBS NPR (July 10, 2020), https://whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/ [https://perma.cc/W5YP-WFJF].

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] Saenz, *supra* note 13, at 806-10.

[129] *Id.* at 811.

[130] *See infra* Section VII.

V. CREATOR LIABILITY

Legislation and legal scholarship most often address NCII through creator liability via state laws and advocating for establishing a federal right of publicity.

A. State Actions

States have increasingly taken action to hold creators liable for using deepfake technology to create pornographic content.[131] Some states have passed laws that outlaw distributing deepfake pornography, some afford the victims the right to sue the creator in civil court, often looking towards current state tort laws,[132] others have criminalized the conduct, and some are considering laws requiring a digital watermark be present on any posted deepfake.[133] For example, a 2023 Louisiana criminal statute allows for the prosecution of any individual that knowingly creates, possesses, or distributes a pornographic deepfake that includes a minor and of any individual that knowingly promotes, distributes, or exchanges a deepfake with knowledge that it's a nonconsensual deepfake, regardless of the age of the individual depicted.[134]

In Pennsylvania, in December 2024, state criminal charges were filed against two Lancaster, PA teenage boys.[135] They were charged by the Lancaster County District Attorney's Office "with one count of criminal conspiracy, fifty-nine counts of sexual abuse of children, fifty-nine counts of dissemination of photographs, fifty-nine counts of possession of child pornography, one count of dissemination of obscene materials to minors, one

---

[131] NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 110.

[132] *E.g.*, Cassandre Coyer, *States Are Targeting Deepfake Pornography But Not in a Uniform Way*, LAW.COM (Aug. 10, 2023), https://www.law.com/legaltechnews/2023/08/10/states-are-targeting-deepfake-pornography-but-not-in-a-uniform-way/ [https://perma.cc/W8KK-AA98]; Saenz, *supra* note 13, at 795-98 (discussing attempts to apply state tort laws to creators of nonconsensual deepfake pornography include defamation, intentional infliction of emotional distress, and false light invasion of privacy); Safaryn, *supra* note 17, at 285-88.

[133] *E.g.*, NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 110; Joey Cappelletti & Ali Swenson, *Michigan to join state-level effort to regulate AI political ads as federal legislation is pending*, PBS (Nov. 29, 2023), https://www.pbs.org/newshour/politics/michigan-to-join-state-level-effort-to-regulate-ai-political-ads-as-federal-legislation-is-pending [https://perma.cc/6V74-BZT2]; Danielle F. Bass & Nathaniel Penning, *The Legal Issues Surrounding Deepfakes*, THE MATRIX HONIGMAN L. FIRM (July 25, 2023), https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes [https://perma.cc/3MHJ-5EDY].

[134] La. Stat. Ann. § 14:73.13.

[135] *Two Juveniles Charged in Connection to AI-Generate Images of Lancaster Country Day School Students; DA Determines School Officials Were Not Legally Required to Report AI Incidents*, LANCASTER CNTY. DIST. ATT'Y'S OFF. (Dec. 5, 2024), https://lancaster.crimewatchpa.com/da/11617/post/2-juveniles-charged-connection-ai-generated-images-lancaster-country-day-school-students [https://perma.cc/BCR7-QR3R].

count of criminal use of a communication facility, fifty-nine counts of possession of obscene materials depicting a minor and one count of possession of obscene materials."[136] It is unknown how the court handled the case because the boys were charged in juvenile court and those cases are not usually a matter of public record.[137]

Most recently, in 2025, New Jersey enacted A3540/S2544 "establishing civil and criminal penalties for the production and dissemination of deceptive" deepfakes.[138] Although state legislatures are increasingly providing remedies for the victims of NCII, it is not enough. There is state-to-state variation in the current laws, "from the language used to define the deepfake, to the type of liability they impose."[139] With the enactment of the TAKE IT DOWN Act, the federal government may finally hold creators responsible. Thankfully, the Act "does not preempt state law" and victims retain the right to redress their harms through state action.[140]

B. Federal Right of Publicity

Some recent proposals to address NCII focus on the development of a federal right of publicity under intellectual property law.[141] "Currently, no federal law governs the right of publicity, and [many] states do not recognize the right at all."[142] However, the United States would not be the first nation to attempt to tackle the problem of NCII through expanding the right to one's own image. German law provides a *general right of responsibility* that "grants individuals the right to their own image . . . [and] essentially renders deepfakes of individuals without consent illegal in Germany."[143] Denmark recently introduced a bill to expand copyright law protections by giving people a fundamental right to their voice, facial features, and "mak[ing] it illegal to share most deepfake images of another person without their consent."[144] Additionally, the law allows individuals to demand social media

---

[136] *Id.*

[137] Ashley Stalnecker, *Where does the Lancaster County Day School case stand now?*, LNP LANCASTER ONLINE (Dec. 26, 2024), https://lancasteronline.com/news/local/where-does-the-lancaster-country-day-school-case-stand-now/article_1be96110-c3d4-11ef-9d7b-0bd4c3bb8449.html. [https://perma.cc/57G9-74XN].

[138] *Law Enacts Civil and Criminal Penalties for Deceptive AI Deepfakes*, N.J. BUS. MAG. (Apr. 2, 2025), https://njbmagazine.com/njb-news-now/law-enacts-civil-and-criminal-penalties-for-deceptive-ai-deepfakes/ [https://perma.cc/US5Q-KNLU].

[139] Coyer, *supra* note 132; *see* Song, *supra* note 13, at 195.

[140] Stuart D. Levi & Mana Ghaemmaghami, *'Take It Down Act' Requires Online Platforms To Remove Unauthorized Intimate Images and Deepfakes When Notified*, SKADDEN (June 10, 2025), https://www.skadden.com/insights/publications/2025/06/take-it-down-act. [https://perma.cc/C8YV-F63B].

[141] *See* H.R. 6943; Asher, *supra* note 13, at 124; Drinkwater, *supra* note 118, at 120.

[142] Saenz, *supra* note 13, at 799.

[143] Quirk, *supra* note 68.

[144] Nierenberg, *supra* note 68.

removal of digital forgeries.[145] However, establishing a federal right of publicity in the United States, that protects the average person, requires expanding who may seek recourse under the law compared to current individual state interpretations.[146]

The right of publicity has origins from New York state law enacted in 1903 under a right of privacy.[147] Today, the right of publicity is a creation of state law and does not provide consistent protections state-to-state.[148] The Second Circuit coined the term "right of publicity" in the 1953 case *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc*.[149] In that case, the Court determined that the right of publicity provided economic protections due to the commercial value of publishing an individual's name or likeness.[150] Therefore, an individual may use the right to "recover damages for the economic value of a defendant's unauthorized exploitation of a plaintiff's name or likeness."[151] The Supreme Court first addressed the right of publicity in the 1977 case *Zacchini v. Scripps-Howard Broadcasting Co*.[152] The Court upheld Ohio's right of publicity law and found that the protection is rooted in "the rationale . . . of preventing unjust enrichment . . ."[153]

Historically, states have taken different routes to provide right of publicity protections. Some states established the right through statutory implementation and others through common law.[154] Although the state-by-state differentiation causes a lack of uniformity in the application of the right, there is consistency in the right protecting a well-known person's financial interest in preventing another from receiving an economic benefit from the use and exploitation of the person's identity.[155] Consequently, without the removal of the well-known person and economic benefit components, remedies for harms from NCII would be limited to those individuals who

---

[145] *Id.*

[146] *See, e.g.*, Saenz, *supra* note 13, at 799; Armand J. (A.J.) Zottola & Channing D. Gatewood, *The Right of Publicity*, VENABLE LLP, (2023), https://www.venable.com/insights/publications/ip-quick-bytes/the-right-of-publicity [https://perma.cc/688C-TMEX]; Asher, *supra* note 13, at 109; Drinkwater, *supra* note 118, at 116; Kevin L. Vick & Jean-Paul Jassy, *Why a Federal Right of Publicity Statute is Necessary*, 28 COMMC'NS L. 14, 15 (2011), https://www.americanbar.org/content/dam/aba/publications/communications_lawyer/august2011/why_fedefed_right_publicity_statute_is_necessary_comm_law_28_2.authcheckdam.pdf [https://perma.cc/Q8KK-3JV8].

[147] Asher, *supra* note 13, at 109.

[148] *Id.*; Vick & Jassy, *supra* note 146, at 14.

[149] Haelan Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953).

[150] *Id.*; Vick & Jassy, *supra* note 146, at 14; Asher, *supra* note 13, at 109.

[151] Vick & Jassy, *supra* note 146, at 14.

[152] Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 576 (1977).

[153] *Id.*; Asher, *supra* note 13, at 109; *see* Vick & Jassy, *supra* note 146, at 15.

[154] *Right of Publicity*, JOHNSON & MARTIN, P.A., https://www.johnsonmartinlaw.com/intellectual-property/right-of-publicity/ [https://perma.cc/4KNC-63MX] (last visited Dec. 7, 2024).

[155] Zottola & Gatewood, *supra* note 146, at 15; *see, e.g.*, Saenz, *supra* note 13, at 799; Asher, *supra* note 13, at 109; Drinkwater, *supra* note 118, at 127; Vick & Jassy, *supra* note 146, at 18.

gain monetary benefits from the use of their identity such as celebrities, adult entertainment workers, or social media influencers.

Unfortunately, a 2024 legislative attempt to develop a federal right of publicity, the No Artificial Intelligence Fake Replicas And Unauthorized Duplications Act (No AI FRAUD Act), gained no traction in Congress.[156] However, it provides a valuable illustration of what a federal right of publicity may need to incorporate to protect a wide breadth of individuals seeking a private right of action to sue a creator of NCII. The No AI FRAUD Act would have established an intellectual property right for every individual in their own likeness and voice that is freely transferable and descendible.[157]

The No AI FRAUD Act would not have limited the right solely to well-known individuals and would have defined an individual as a human being, living or dead.[158] The legislation did not prohibit deepfake creation altogether, instead, Section 3(b)(4) would have allowed individuals to purposefully contract for the use of their digital depiction or digital replica for novel performances in an advertisement or expressive work.[159] This preserves artists and advertisers First Amendment rights and interests in creative expression and provides individuals, including social media influencers, celebrities, and adult entertainment workers, a means to contract with compensation for the use of their depiction or voice in deepfake media.

The No AI FRAUD Act also built in First Amendment protections as a defense under Section 3(d).[160] A defendant would have been able to raise an affirmative defense under the First Amendment using a balancing test weighing "the public interest in access to the use . . . [and] the intellectual property interest in the voice or likeness."[161] Importantly, it would have provided multiple balancing tests for courts to weigh the costs and benefits to each party and preserve the creative and expressive rights of individuals while also prioritizing the harm caused to the victim.[162] The No AI FRAUD Act would have covered a wide range of harms under section 3(e)(2), including financial, physical, severe emotional distress, and likelihood of deception.[163] Additionally, it would have established per se harm as protection for minors that are victims of NCII under Section 3(e)(3).[164]

While the No AI FRAUD Act would have given broad federal intellectual property rights to all individuals under the right of publicity, it still would not have resolved the problem of ensuring swift removal of NCII

---

[156] H.R. 6943.
[157] *Id.* § 3(b)(1)-(3).
[158] *Id.* § 3(a)(1).
[159] *Id.* § 3(b)(4).
[160] *Id.* § (3)(d).
[161] *Id.*
[162] *See id.*
[163] *Id.* § 3(e)(2).
[164] *Id.* § 3(e)(3).

from social media platforms.[165] The ability to request removal of a harmful image with the expectation of compliance by the platform helps protect victims in ways that are less costly than suing creators.[166] In an age where personal data, including an individual's image, is weaponized disproportionately against women and LGBTQ+ individuals, federal protections, like the TAKE IT DOWN Act, help provide a standard, unified approach to safeguard victims.[167]

VI. PASSING THE TAKE IT DOWN ACT

Senators Cruz (R-TX) and Klobuchar (D-MN) first introduced the TAKE IT DONW Act in the United States Senate as S.4569 in April 2024, during the 118th Congress.[168] Shortly thereafter, in June of 2024, the bill was introduced by Representatives Salazar (R-FL) and Dean (D-PA) in the House as H.R.8989.[169] The Senate committee hearings on the bill included survivor testimony and statements of support from various organization.[170] These hearings were persuasive enough to acquire bipartisan support by September of 2024.[171] The Senate passed S.4569 in December 2024; however, it was not enough to move the bill towards enactment prior to the end of the 118th Congressional Session.[172]

In January 2025, as the 119th Congress began, the TAKE IT DOWN Act was reintroduced in the Senate and House as S.146 and H.R.633 respectively.[173] On February 13, 2025, the TAKE IT DOWN Act passed the United States Senate by unanimous consent highlighting the receipt of "widespread support from over 100 organizations, including victim advocacy groups, law enforcement, and tech industry leaders."[174] On April 28, 2025, the United States House of Representatives passed the TAKE IT

---

[165] One of the things the TAKE IT DOWN Act does provide is a way to get these images removed from platforms and, hopefully, hold covered platforms accountable if they do not comply within the stipulated time frame. However, it is not clear how much leeway covered platforms will be given under the good-faith limitation on liability. *See* 47 U.S.C. §§ 223a(a)(4).

[166] Pavlina Pavlova, *The Digital War on Women: Sexualized Deepfakes, Weaponized Data and Stalkerware That Monitors Victims Online*, MS. MAG. (Nov. 21, 2024), https://msmagazine.com/2024/11/21/women-online-harrassment-abuse-deepfake-violence-revenge-porn/ [https://perma.cc/HT2Y-ZDEA]; *Cruz-Klobuchar Bill to Protect Teenagers*, *supra* note 8.

[167] Pavlova, *supra* note 166.

[168] *TAKE IT DOWN Act*, RAINN, https://rainn.org/federal-legislation/take-it-down-act/ [https://perma.cc/5H5H-BBT6] (last visited Sep. 8, 2025).

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] *Id.*

[174] *Cruz-Klobuchar Bill to Protect Teenagers*, *supra* note 8.

DOWN Act by a vote of 409-2.[175] Less than a month later, on May 19, 2025, the TAKE IT DOWN Act was signed into law.[176]

The TAKE IT DOWN Act is the first federal law to directly criminalize both the distribution of NCII and threats to publish NCII.[177] The Act demands swift removal of NCII from covered platforms.[178] Importantly, the Act also protects victims, law enforcement officials, and individuals assisting law enforcement from penalties for any disclosures of NCII.[179] This Note argues that while the Act's enactment is an important milestone in federal legislation, it is an incomplete way to provide recourse to victims of NCII. Therefore, victims should use additional federal pathways, in conjunction with the TAKE IT DOWN Act, to address harms.

VII. THREE FEDERAL PATHWAYS

This Note offers three federal pathways to help NCII victims reclaim their image and address the harms associated with the creation and distribution of NCII. First, victims may rely on the government to file criminal charges under Section 2 of the TAKE IT DOWN Act.[180] Second, victims should use the private right of action provisions under VAWA relating to the disclosure of intimate images[181] and under the CPPA relating to the sexual exploitation of children.[182] Third, victims should request removal of any images found on covered platforms under Section 3, Notice and Removal of Nonconsensual Intimate Visual Depictions, of the TAKE IT DOWN Act.[183] This Note argues that these three pathways should be used in conjunction with each other to hold the greatest number of creators, distributors, and platforms accountable within the current federal legal framework.

---

[175] Press Release, U.S. Senate Comm. Com., Sci., & Transp., TAKE IT DOWN Act Passes the House, Heads to President Trump's Desk (Apr. 28, 2025) [hereinafter TAKE IT DOWN Act Passes the House], https://www.commerce.senate.gov/2025/4/take-it-down-act-passes-the-house-heads-to-president-trump-s-desk [https://perma.cc/SB8T-2W2J].

[176] TAKE IT DOWN Act Signed into Law, *supra* note 38.

[177] *Legislation TAKE IT DOWN Act Criminalizes Non-Consensual Intimate Images (NCII)*, RAINN [hereinafter *Legislation TAKE IT DOWN Act*], https://rainn.org/policy/take-it-down-act [https://perma.cc/BJR2-89GH] (last visited March 17, 2025); Sundberg, *supra* note 4, at 1209.

[178] *Legislation TAKE IT DOWN Act*, *supra* note 177.

[179] *Id.*; 47 U.S.C. § 223(h)(3)(C).

[180] 47 U.S.C. § 223(h).

[181] 15 U.S.C. § 6851.

[182] 18 U.S.C. § 2252(A)(f).

[183] 47 U.S.C. § 223a.

A. TAKE IT DOWN Act Section 2

Section 2 of the TAKE IT DOWN Act federally criminalizes the intentional disclosure of nonconsensual intimate visual depictions.[184] The Act purposefully criminalizes both "authentic intimate visual depictions"[185] as well as "digital forgeries"[186] involving adults and minors.[187] The Act defines a "digital forgery" as:

> [A]ny intimate visual depiction[188] 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.[189]

While the Act distinguishes between adult and minor victims, the underlying language remains the same.[190] The two subsections make it "unlawful for any person, in interstate or foreign commerce, to use an interactive computer service to knowingly publish a digital forgery of an identifiable individual[.]"[191]

The requirements for offenses against adults are more intricate than those for offenses against minors.[192] Violations involving adults requires that:

> (i) the digital forgery was published without the consent of the identifiable individual;
>
> (ii) what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting;
>
> (iii) what is depicted is not a matter of public concern; and

---

[184] *Id.*; Sundberg, *supra* note 4, at 1218.

[185] 47 U.S.C. § 223(h)(2). It is outside the scope of this Note to provide a detailed discussion on authentic intimate visual depictions. This Note focuses strictly on deepfake nonconsensual intimate visual depictions produced with the use of computer or other technological means.

[186] *Id.* § 223(h)(3).

[187] *Id.* § 223(h)(2)-(3).

[188] The definition of "intimate visual depiction" in the TAKE IT DOWN Act comes from 15 U.S.C. § 6851 defined, in part, as "a visual depiction, as that term is defined in 18 U.S.C. § 2256(5), that depicts the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual." In turn, the definition of "visual depiction" in 18 U.S.C. § 2256(5) covers, in part, "data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format."

[189] 47 U.S.C. § 223(h)(1)(B).

[190] Sundberg, *supra* note 4, at 1221.

[191] 47 U.S.C. §§ 223(h)(3)(A), (B).

[192] *See* Sundberg, *supra* note 4, at 1222.

(iv) publication of the digital forgery –

(I) is intended to cause harm; or

(II) causes harm, including psychological, financial, or reputational harm, to the identifiable individual.[193]

The offense for digital forgeries involving minors does not share any of the requirements for cases involving adults.[194] Violations involving minors require "intent to – (i) abuse, humiliate, harass, or degrade the minor; or (ii) arouse or gratify the sexual desire of any person."[195]

Notably, the Act includes exceptions which bar the application of offenses for digital forgeries.[196] The exceptions include protections for disclosures of digital forgeries to assist in reports made to law enforcement for investigations, and protective or intelligence activity, those made in good faith, including those to help an identifiable individual, and possession or publication of digital forgeries of yourself.[197] The Act also includes an exception for intimate visual depictions that qualify as child pornography or sexual abuse of children under 18 U.S.C. § 2256 and 18 U.S.C. §§ 1466A(a)-(b) respectively.[198]

Under the TAKE IT DOWN Act, offenses of digital forgeries must include an "identifiable individual." This aligns with prior case law differentiating between virtual child pornography and morphed child pornography.[199] An identifiable individual is "an individual (i) who appears in whole or in part in an intimate visual depiction; and (ii) whose face, likeness, or other distinguishing characteristic . . . is displayed in connection with such intimate visual depiction."[200]

While the Section 2 of the TAKE IT DOWN Act can be a powerful tool for the government, a civil private right of action is missing and consequently, the TAKE IT DOWN Act does not close the gaps on all possible recovery measures for victims.[201] However, there are current federal laws that victims may be able to utilize as a remedy for the lack of a private right of action.[202]

---

[193] 47 U.S.C. § 223(h)(3)(A).

[194] Sundberg, *supra* note 4, at 1222.

[195] 47 U.S.C. § 223(h)(3)(B).

[196] *Id.* § 223(h)(3)(C).

[197] *Id.* § 223(h)(3)(C)(i)-(iv).

[198] The inclusion of this language is presumably to preserve the sentencing scheme under 18 U.S.C. § 2256 and 18 U.S.C. §§ 1466A(a)-(b) to avoid a conflict of law. *See* 47 U.S.C. § 223(h)(3)(C)(v).

[199] *See infra* section VII(B).

[200] 47 U.S.C. §§ 223(h)(1)(C)(i)-(ii).

[201] *See* Saenz, *supra* note 13, at 810 ("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").

[202] *See* 15 U.S.C. § 6851; 18 U.S.C. § 2252A(f); *cf.* Pascale, *supra* note 1, at 363-65 (recommending Congress look to 18 U.S.C. 2252A(a) and 2256(8)(C) when constructing legislation to address deepfake

B. CPPA & VAWA

This Note argues victims of NCII can, and should, sue creators in civil court under 18 U.S.C. § 2252A of the Child Pornography Prevention Act of 1996 (CPPA), 15 U.S.C. § 6851 of the 2022 Reauthorization of the Violence Against Women Act (VAWA), or both, depending on the age of the victim. However, it is important to acknowledge that individuals are often unable to pursue civil right of action remedies because they are frequently cost prohibitive, time consuming, public, and do not provide any guarantee of a decision in favor of the victim and may be "moot against a judgement-proof offender."[203]

First Amendment free speech[204] applications to pornographic material have long relied on an evaluation of whether the material a state is seeking to regulate qualifies as obscene.[205] The United States Supreme Court has found that First Amendment free speech protections do not always extend to pornographic or obscene material.[206] In *Miller v. California*, the United States Supreme Court established a three-part test that must be satisfied to determine that the pornographic or obscene material in question is not granted First Amendment free speech protection.[207]

> Under the three-part *Miller* test, the trier of fact must first determine whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest. Next, the trier of fact must determine whether the material depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law. Finally, the trier of fact must determine whether the work lacks serious literary, artistic, political, or scientific value.[208]

In *Ashcroft v. Free Speech Coalition*, the Supreme Court of the United States examined portions of the CPPA using the *Miller* test and struck down portions of the law.[209] The Court found that the portion of the CPPA related to virtual child pornography failed the three-part *Miller* test and held that virtual child pornography is protected speech under the First Amendment.[210]

---

pornography because courts have upheld this language related to morphed child pornography multiple times and this would help avoid challenges for overbroad definitions).

[203] Sundberg, *supra* note 4, at 1220.

[204] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech.").

[205] *See* Safaryn, *supra* note 17, at 283-84.

[206] *See id.*; Roth v. United States, 354 U.S. 476, 484-85 (1957); Miller v. California, 413 U.S. 15, 25 (1973). *But see* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 259 (2002).

[207] *See Miller*, 413 U.S. at 25; Safaryn, *supra* note 17, at 283-84.

[208] Safaryn, *supra* note 17, at 283-84 (internal quotations omitted).

[209] *Free Speech Coalition*, 535 U.S. at 257.

[210] *Id.* at 251; *see* Safaryn, *supra* note 17, at 291.

Virtual child pornography is the creation of "realistic images of children who do not exist."[211]

However, "federal courts have generally upheld convictions for possession of morphed child pornography."[212] Morphed child pornography is "alter[ing] innocent pictures of real children so that the children appear to be engaged in sexual activity."[213] The use of real children in morphed or AI generated pornographic images is more akin to the production of child pornography without virtual modification because it involves "the interests of real children."[214] Courts have found that "[g]overnments have a compelling interest in protecting children from child pornography and are afforded considerable leeway in regulating those aspects of the child pornography market that are intrinsically related to the harm that child pornography inflicts on children."[215]

For example, in *United States v. Hotaling*, the Second Circuit held "that child pornography created by digitally altering sexually explicit photographs of adults to display the face of a [real] child is not protected expressive speech under the First Amendment."[216] The court looked to the Supreme Court cases *Free Speech Coalition* and *New York v. Ferber* to support the interpretation that the primary concern is the protection and prevention of harm to children.[217] In *Ferber*, the Supreme Court acknowledged that the harms of child pornography extend beyond the initial creation because of fears and concerns related to the sustained circulation of the images.[218] In *Hotaling*, the Second Circuit identified the ultimate question that courts should ask when addressing federal criminal prosecutions under 18 U.S.C. § 2252A of morphed child pornography, "whether an image of child pornography implicates the interests of an actual minor?"[219]

It is likely that courts will hold that the First Amendment does not protect the creation of NCII deepfakes of real children.[220] The protection of the interests of minor victims of NCII provides tangible criminal consequences for creators, even if those creators are also minors. While it may be very rare to charge a minor with a violation under sections of 18 U.S.C. §§ 2251-2260A, the court in *United States v. Streett* held that the statute does not

---

[211] *Free Speech Coalition*, 535 U.S. at 240.

[212] Safaryn, *supra* note 17, at 291.

[213] *Free Speech Coalition*, 535 U.S. at 242.

[214] *Id.*

[215] United States v. Streett, 434 F. Supp. 3d 1125, 1181 (D.N.M. 2020); *See* New York v. Ferber, 458 U.S. 747, 778 n. 10 (1982).

[216] United States v. Hotaling, 634 F.3d 725, 726 (2nd Cir. 2011).

[217] *Id.* at 728; *Free Speech Coalition*, 535 U.S. at 249; *Ferber*, 458 U.S. at 759 n. 10.

[218] *Ferber*, 458 U.S. at 759.

[219] *Hotaling*, 634 F.3d at 729.

[220] *See* United States v. Mecham, 950 F.3d 257, 260 (5th Cir. 2020); United States v. Anderson, 759 F.3d 891, 893 (8th Cir. 2014); *Hotaling*, 634 F.3d at 726; United States v. Bach, 400 F.3d 622, 629 (8th Cir. 2005).

exclude minors, and that the statute does not limit charges to the government seeking criminal liability.[221] It is likely that courts would extend criminal protections to NCII deepfake victims that are minors under portions of 18 U.S.C. §§ 2251-2260A given the treatment of prior cases of morphed child pornography.[222] Therefore, a minor that creates NCII deepfake images, like those in Westfield, NJ or Lancaster, PA, could be charged under sections of 18 U.S.C. §§ 2251-2260A.

The intimate visual depiction definition under 15 U.S.C. § 6851(a)(5) of VAWA also likely covers NCII because victims are identifiable by their face and artificially appear nude depicting the sexually explicit covered content.[223] The statute does not require that the depicted individual engaged in the intimate visual depiction in real life.[224] However, VAWA does require that the victim's "body appears in whole or in part in an intimate visual depiction."[225] Therefore, to succeed on a claim under the revenge porn VAWA provision, victims must persuade the court that the retention of only their face in an NCII deepfake is enough to meet the requirement of part of their body appearing in the intimate visual depiction.[226] This Note argues that, like findings under 18 U.S.C. § 2252A, courts are likely to hold that 15 U.S.C. § 6851 protects NCII victims and find that NCII deepfake images retaining just the face of a victim fall under the revenge porn VAWA provision because of the real harms victims incur.[227]

Unfortunately, courts have not yet reached decisions regarding the treatment of NCII under 15 U.S.C. § 6851.[228] However, in 2024, one of the girls from Westfield, NJ high school filed a lawsuit against one of her classmates that created and shared her image in a pornographic nonconsensual deepfake.[229] The student is requesting civil relief under "the Violence Against Women Reauthorization Act (15 U.S.C. § 6851), the Federal Child Pornography and Abuse Statutes (18 U.S.C. § 2252A), New Jersey's non-consensual pornography statute (NJSA § 2A:58D-1), and state

---

[221] United States v. Streett, 434 F. Supp. 3d 1125, 1176 (D.N.M. 2020); *see* 18 U.S.C. § 2252A(f); *accord* Complaint Summons & Civil Cover Sheet at 1, Doe v. Smith, 2:24-cv-00634 (D.N.J. Feb. 2, 2024), ECF No. 1; Oral Decision on Motion for TRO at 2, Doe v. Smith, 2:24-cv-00634 (D.N.J. Feb. 15, 2024), ECF No. 26.

[222] *Mecham*, 950 F.3d at 260; *Anderson*, 759 F.3d at 893; *Hotaling*, 634 F.3d at 726; *Bach*, 400 F.3d 622.

[223] 15 U.S.C. § 6851(a)(5).

[224] *See* Safaryn, *supra* note 17, at 294.

[225] 15 U.S.C. § 6851(a)(3).

[226] *See* Safaryn, *supra* note 17, at 294.

[227] *See supra* Section II (discussing reputational, physical, mental, and financial harms faced by victims).

[228] It is possible that settlements occurred in previous attempts to hold nonconsensual deepfake pornography creators civilly liable under 15 U.S.C. § 6851.

[229] Complaint Summons & Civil Cover Sheet at 1, Doe v. Smith, 2:24-cv-00634 (D.N.J. Feb. 2, 2024), ECF No. 1.

common law tort theories of liability."[230] The case is ongoing.[231] If *Doe v. Smith* does not reach a settlement agreement, it may be the first court decision to establish a precedent of applying 15 U.S.C. § 6851 to nonconsensual deepfake pornography.

Unlike the TAKE IT DOWN Act, 15 U.S.C. § 6851 and 18 U.S.C. § 2252A(f) provide adult and minor victims with the ability to sue creators for civil remedies through a private right of action.[232] Individual victims can still seek civil remedies for nonconsensual intimate imagery under some state "privacy tort laws like false light, defamation, or intentional infliction of emotional distress."[233] However, the variability between states makes this a complicated solution.[234] Therefore, utilizing the CPPA and VAWA federal provisions removes the concern for inconsistency in application between states, protects all victims regardless of age, and does not require reliance on federal enforcement of the TAKE IT DOWN Act. Despite this Note's recommendation, pursuing cases under 18 U.S.C. § 2252A and 15 U.S.C. § 6851 may be cost prohibitive and victims deserve cost-effective removal options for NCII.

C. TAKE IT DOWN Act Section 3

The TAKE IT DOWN Act provides individuals with an actionable power to request removal of an NCII image from online platforms.[235] Requesting removal is more cost efficient than suing the individuals that create and distribute the NCII.[236] If online platforms do not comply with removal, the Federal Trade Commission should enforce adherence by covered platforms under Section 3(b).[237] Section 3 of the TAKE IT DOWN Act should be challenged in court to define the scope of "good faith" under Section 3(a)(4) and determine the constitutionality of Section 3 in light of Section 230.

Section 3 of the TAKE IT DOWN Act sets standards for the notice and removal of nonconsensual intimate visual depictions.[238] The section establishes that, within one year of enactment, covered platforms[239] must

---

[230] *Id.*

[231] Docket Report, Doe v. Smith, No.2:24-cv-00634 (D.N.J. Mar. 21, 2025).

[232] 15 U.S.C. § 6851; 18 U.S.C. § 2252A(f).

[233] Coyer, *supra* note 132; *see* Saenz, *supra* note 13, at 795-98.

[234] Coyer, *supra* note 132.

[235] 47 U.S.C. § 223a.

[236] *Cruz-Klobuchar Bill to Protect Teenagers*, *supra* note 8.

[237] 47 U.S.C. § 223a(b).

[238] *Id.* § 223a(a)(1)-(3).

[239] TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 61 ("means a website, online service, online application, or mobile application (i) that serves the public; and (ii)(I) that primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files; or (II) for which it is in the regular course of trade or business of the website, online service, online application, or mobile application to publish, curate, host, or make available content of nonconsensual intimate visual

develop procedures for victims to provide a notification to the platform that a nonconsensual pornographic image was published on the platform and provide a process for requests for removal of that image.[240] Platforms are required to offer "a clear and conspicuous notice . . . and removal process" that outlines openly and simply the procedure established by that covered platform to notify and request removal.[241] The covered platform has forty-eight hours after submission of an acceptable request for removal to "remove the intimate visual depiction and make reasonable efforts to identify and remove any known identical copies of such depiction."[242]

Advocates of the bill, argued "[t]he bill is narrowly tailored to criminalize knowingly publishing NCII without chilling lawful speech."[243] Maintaining that courts will likely find that the bill does not violate First Amendment rights because it requires "that computer-generated NCII meet a 'reasonable person' test for appearing indistinguishable from an authentic image."[244] Conversely, those in opposition to the law argued that it is probably unconstitutional, and will "[threaten] free expression, user privacy, and due process, without addressing the problem it claims to solve."[245] Until the constitutionality is determined by the courts, if platforms fail to implement and provide a clear and specific pathway to get NCII images removed from covered platforms, the Federal Trade Commission must enforce any failures to adhere.

CONCLUSION

NCII is a growing, but not novel, phenomenon. The negative impact is wide-reaching with instances impacting notable female celebrities, politicians, adult entertainment workers, and most disastrously, children.[246] Scholars have proposed a variety of solutions and Congress has introduced multiple legislative attempts over the last nine years, yet no substantial federal legislation passed until the TAKE IT DOWN Act. Many states took

depictions"). As of the time of this publication this definition section has not been codified in the U.S. Code.

[240] *Id.* § 223a(a)(1)(B).

[241] *Id.* § 223a(a)(2).

[242] *Id.* § 223a(a)(3).

[243] *Cruz-Klobuchar Bill to Protect Teenagers*, *supra* note 8.

[244] *Id.*

[245] India McKinney, *The Senate Passed The TAKE IT DOWN Act, Threatening Free Expression and Due Process*, EFF (Feb. 25, 2025), https://www.eff.org/deeplinks/2025/02/senate-passed-take-it-down-act-threatening-free-expression-and-due-process [https://perma.cc/C28X-X2T7]; *see* Kaylee Williams, *Free Speech Advocates Express Concerns As TAKE IT DOWN Act Passes US Senate*, TECH POLICY PRESS (Feb. 21, 2025), https://www.techpolicy.press/free-speech-advocates-express-concerns-as-take-it-down-act-passes-us-senate/ [https://perma.cc/2Y62-S9BY].

[246] *See supra* Section II.

action and passed legislation to address NCII in a variety of ways.[247] However, state solutions are not uniform and may cause jurisdictional problems if the creator and target are not within the jurisdictional bounds of the same state.[248] This Note argues that the best current federal solution to address the harms associated with NCII is utilizing the TAKE IT DOWN Act, 18 U.S.C. §§ 2251-2260A, and 15 U.S.C. § 6851.

Critiques of this Note may point out that these are all reactive measures and are not preventive measures to stop the sharing and creation of nonconsensual deepfake pornography ahead of the harm inflicted on victims.[249] Consequently, future research should build on the proposed solution of establishing public-private partnerships with social media platforms and deepfake software applications.[250] While imposing liability may be an incentive for platforms to modify their procedures, the lobbying power of social media and AI platforms may derail any substantial effort proposed by Congress.[251] Therefore, providing incentives through federal grants or tax-breaks, as recommended in earlier scholarship, may drive platforms to willingly protect individuals from NCII deepfake harms.[252]

Despite how beneficial preventive measures would be, laws providing avenues for criminal and civil penalties for creators are equally, if not more, important than preventive measures because many people are already living with the negative impact of NCII and deserve an avenue for redress through the legal system. This Note argues that the federal government should use Section 2 of the TAKE IT DOWN Act to hold creators of NCII images liable.[253] Additionally, this Note recommends that, even though the TAKE IT DOWN Act does not have a civil cause of action provision, victims should sue under either 15 U.S.C. § 6851, 18 U.S.C. § 2252A, or both depending on the age of the target. Lastly, this Note suggests that NCII victims should use Section 3 of the TAKE IT DOWN Act to request removal of images from covered platforms.[254] Requesting removal provides victims with a cost-effective way to mitigate the harms associated with covered platforms continuing to carry NCII images of their likeness. Using all three federal pathways provides consistency in application across all states and allows victims to seek redress from both creators and platforms.

---

[247] Coyer, *supra* note 132; Saenz, *supra* note 13, at 800-804.

[248] *See* Chesney & Citron, *supra* note 51, at 1792.

[249] *See* Song, *supra* note 13, at 216-22.

[250] *See id.*

[251] *See id.* at 215; Stephen J. Dubner, FREAKONOMICS RADIO: *How to Poison the A.I. Machine* (Apple Podcasts, Jan. 24, 2025), https://freakonomics.com/podcast/how-to-poison-an-a-i-machine/ [https://perma.cc/6M93-QFYB].

[252] *See* Song, *supra* note 13, at 216-22.

[253] 47 U.S.C. § 223.

[254] *Id.* § 223a.