FROM CONSENT TO CONTROL: REDEFINING LEGAL AUTONOMY IN THE AGE OF DEEPFAKE PORNOGRAPHY WITH A POST-CONSENT FRAMEWORK

SHANNON STALL*

> And I really feel like my whole world fell apart at that moment. . . . You have to look at how many views are there, and how many people have violated you. I just didn't want to live anymore, because the shame was too, too much for me to bear.
>
> – Breeze Liu.[1]

INTRODUCTION

Ms. Liu describes when "a friend discovered her face superimposed on pornographic images."[2] She, like 143,733 people and counting,[3] was a victim[4] of deepfake pornography.[5] Deepfake—a portmanteau of "deep learning" and "fake"—refers to synthetic image, audio, or video representations of individuals generated using machine learning

---

* Associate Managing Editor, *Jurisprudence Review*, vol. 18; J.D. Candidate, Washington University School of Law, Class of 2026. All views expressed are my own. A special thank you to my family and my partner Lane for their unwavering love and support, and to my mentor, Rob, whose guidance brought me to law school and whose example I aspire to follow.

1. *See* Jo Ling Kent et al., *Lawmakers Pursue Legislation that Would Make it Illegal to Share Digitally Altered Images Known as Deepfake Porn*,CBS NEWS (May 23, 2024), https://www.cbsnews.com/news/legislation-share-deepfake-porn-images-crime/.

2. *Id.*

3. *See* Nurudeen Akewushola, *Nearly 4,000 Celebrities Are Victims of Deepfake Pornography—Report*, FACTCHECKHUB (March 22, 2024), https://factcheckhub.com/nearly-4000-celebrities-are-victims-of-deepfake-pornography-report/ ("In the first three-quarters of 2023, over 143,733 new deepfake porn videos were uploaded to the 40 most used deepfake pornography sites.").

4. This Note uses the term "victim" instead of "survivor" to acknowledge that these individuals have experienced a criminal harm. The term "victim" therefore reflects their legal status and the distinct rights afforded to them under law. "However, the word does not imply weakness, assume guilt, or assign blame." *Victim or Survivor? Terminology From Investigation Through Prosecution*, SEXUAL ASSAULT KIT INITIATIVE ("SAKITTA"), https://sakitta.org/toolkit/docs/Victim-or-Survivor-Terminology-from-Investigation-Through-Prosecution.pdf (last visited Feb. 12, 2025). Furthermore, research shows that labeling sexual victimization "cannot be considered a valid criterion for determining who has experienced sexual victimization." Melanie S. Harned, *Does It Matter What You Call It? The Relationship Between Labeling Unwanted Sexual Experiences and Distress*, 72 J. CONSULTING & CLINICAL PSYCH. 1090 (2004).

5. This author agrees with the view of other scholars and advocates that the umbrella term IBSA (image-based sexual assault) is preferred to "deepfake pornography." *See* Cyber Civil Rights Initiative, *Legislative Reform*, https://cybercivilrights.org/legislative-reform/ (last visited Sept. 24, 2025). But, due to its overwhelming prevalence in popular media and scholarship, this Note utilizes the latter term.

techniques.[6] Deepfake technology has become shockingly accessible and capable, leading to a rapid spread in recent years.[7] Today's technology allows the superimposition of images or videos of one person onto the body of another with increasing realism in just a few clicks.[8] The majority of scholarship on deepfakes has centered on the dangers they present in the political sphere, even though the vast majority of deepfakes are pornographic.[9]

Public concern over deepfake pornography first arose when perpetrators weaponized the technology to victimize female celebrities.[10] However, "the rapid advancement and widespread accessibility of AI technology means that anyone who has appeared in a digital image may now 'star' in a pornographic deepfake without their consent."[11] The increased availability of deepfake generators also means that "[a]nyone can create their own deepfake porn images, regardless of their skill level."[12] All you need is an internet connection, and the power of deepfake technology is at your fingertips.

While "anyone whose image has been captured digitally and posted on the internet" can become a victim of deepfake pornography,[13] it is critical

---

6. *See* Mika Westerlund, *The Emergence of Deepfake Technology: A Review*, 9 TECH. INNOVATION MGMT. REV. 16 (2019); *see also* Hany Farid, *Creating, Using, Misusing, and Detecting Deep Fakes*, 1 J. ONLINE TR. & SAFETY 4 (2022).

7. For example, "[t]he total number of deepfake porn videos produced in 2023 increased 464% from 2022." Matthew Lowe, *The Deeply Complicated Issues Surrounding Deepfakes*, N.Y. STATE BAR ASS'N (Feb. 3, 2025), https://nysba.org/the-deeply-complicated-issues-surrounding-deepfakes/.

8. *See* Rex Woodbury, *The Rise of Synthetic Media and Digital Creators*, DIGITAL NATIVE (Apr. 28, 2021), https://www.digitalnative.tech/p/the-rise-of-synthetic-media-and-digital (last visited Oct. 2, 2024); *see also* U.S. Dep't of Homeland Sec., *Increasing Threats of Deepfake Identities* 3 (2023), https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf. ("Deepfakes, an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened.").

9. *See* Emily Pascale, *Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse*, 73 SYRACUSE L. REV. 335, 336 (2023).

10. *See, e.g.*, Nick Statt, *Fake Celebrity Porn Is Blowing Up on Reddit, Thanks to Artificial Intelligence*, THE VERGE (Jan. 24, 2018, 2:53 PM), https://www.theverge.com/2018/1/24/16929148/fake-celebrity-porn-ai-deepfake-face-swapping-artificial-intelligence-reddit; Akewushola, *supra* note 3.

11. Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887, 937 (2019); *see also* U.S. Dep't of Homeland Sec., *supra* note 8, at 10 (noting that "[t]he use of the technology to harass or harm private individuals who do not command public attention and cannot command resources necessary to refute falsehoods should be concerning").

12. *See* Hailey Reissman, *What Is Deepfake Porn, and Why Is It Thriving in the Age of AI?*, UNIV. OF PA. (July 13, 2023), https://www.asc.upenn.edu/news-events/news/what-deepfake-porn-and-why-it-thriving-age-ai (reporting the contents of a question-and-answer interview with University of Pennsylvania Annenberg School for Communication doctoral candidate, Sophie Maddocks, addressing the growing problem of image-based sexual abuse). For a discussion on the financial incentives to produce and disseminate deepfake pornography, see Pascale, *supra* note 9, at 339–40.

13. *See* U.S. Dep't of Homeland Sec., *supra* note 8, at 23–24 (internal quotations omitted).

to recognize "the gendered dimension of the exploitation of deep fakes;"[14] since women are depicted in virtually all posted deepfake pornography.[15] Drawing on cyberfeminism and postmodern legal theory,[16] this Note argues that current legal responses to deepfake pornography are inadequate and that their inadequacy, in large part, stems from the continued use of binary consent-based paradigms.[17]

Deepfakes pose a unique challenge to legal consent frameworks because they allow the creation of explicit content without *any* direct involvement from the victim, effectively rendering the traditional understanding of consent irrelevant.[18] As such, this Note proposes a new framework—the *post-consent framework*—to apply to the issue of deepfake pornography.[19] Such a framework, as the term suggests, moves beyond the idea of a one-time grant of consent and instead emphasizes a need to center legal protections for victims of deepfake pornography on control over their digital identity.[20]

This Note unfolds as follows: Part I explores the various consequences of deepfake pornography on victims, especially for women, both individually and collectively. Part II sets forth the reasons why the current legislation remains inadequate for addressing deepfake pornography. Part III outlines how postmodern legal theory and cyberfeminist critique are essential to reshaping the understanding of consent and autonomy in digital spaces. Part IV introduces the post-consent framework to better address the unique harms posed by deepfake pornography. The potential criticisms of implementing the post-consent framework are also discussed in this section. Part V concludes the Note with a discussion of suggested ways for lawmakers and digital platforms to implement a post-consent framework in the future.

---

14. Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1773 (2019).

15. *See* U.S. Dep't of Homeland Sec., *supra* note 8, at 23 ("95% of deepfakes are of nonconsensual porn of women. Individual level is the highest threat. This number includes anyone whose image has been captured digitally and posted on the internet.") (internal quotations omitted); *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-379SP, SCIENCE & TECH SPOTLIGHT: DEEPFAKES (Feb. 20, 2020), https://www.gao.gov/products/gao-20-379sp ("Deepfakes are usually pornographic and disproportionately victimize women."); *see also State of Deepfakes: Key Findings*, SECURITY HERO, https://www.securityhero.io/state-of-deepfakes/#key-findings (last visited Jan. 26, 2025) ("Deepfake pornography makes up 98% of all deepfake videos online. 99% of the individuals targeted . . . are women.").

16. *See* Part III, *infra*.

17. *See* Part I, *infra*.

18. *Id.*

19. *See* Part IV, *infra*.

20. *Id.*

I. DEEPFAKE PORNOGRAPHY'S GENDERED HARM

Deepfake technology allows perpetrators to make hyper-realistic depictions of victims in sexually explicit simulations. Deepfake pornography reduces individuals—primarily women—to virtual sex objects[21], exemplifying that "if we take 'sexual autonomy seriously,' we will see that the use or threat of physical force is only one of several means by which a woman's right to control her sexuality may be violated."[22] Deepfake pornography represents one such means and should therefore be recognized as a violation of women's sexual privacy, both individually and collectively. Since "victims of deepfakes do not agree to manipulation of their face onto the body of an individual engaging in sexual acts . . . deepfakes . . . violate individuals' expectations that sexual activity be founded on consent."[23]

Deepfake pornography subjects victims to unique kinds of trauma[24] which the law should recognize as harm, whether or not they can "prove" it under currently accepted standards.[25] The trauma can manifest from the loss of control over their image, the fear of public exposure, and the dissonance of seeing themselves in compromising or degrading situations they had no part in.[26] Deepfake pornography can cause significant intangible harms to victims, including anxiety, depression, fear, and isolation.[27] They may also suffer tangible harms, such as damage to their reputation and employment.[28] Some victims have suffered such pervasive invasions of privacy that they were forced to change their names.[29] The dark irony lies in the fact that the victim's "real life" identity had to change due to the harm done to their online identity, illustrating just how greatly the two realities have become intertwined.

---

21. *Id.*

22. *See* Alan Wertheimer, *What Is Consent? And Is It Important?*, 3 BUFF. CRIM. L. REV. 557, 558 (2000) (citing Stephen J. Schulhofer, *Taking Sexual Autonomy Seriously: Rape Law and Beyond*, 11 LAW & PHIL. 35 (1992) and STEPHEN J. SCHULHOFER, UNWANTED SEX: THE CULTURE OF INTIMIDATION AND THE FAILURE OF LAW (1998)).

23. *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1938 (2019) ("Digital technologies enable sexual-privacy invasions that existing law is ill suited to address. Sometimes, law's inadequacy stems from the fact that it has developed in an incremental fashion. At other times, it originates from outmoded assumptions.").

24. *See id.*; Chesney & Citron, *supra* note 14, at 1773 ("When victims discover that they have been used in deep-fake sex videos, the psychological damage may be profound—whether or not this was the video creator's aim.").

25. *See* Pascale, *supra* note 9, at 348 ("Irrespective of whether the video discloses its falsity, the deepfake appropriates one's sexual identity, exhibiting it to the world without consent. Accordingly, the law should protect victims from this unwarranted exposure.").

26. *See* Citron, *supra* note 23, at 1924–28.

27. *Id.* at 1926–27.

28. *Id.*

29. *See* Citron, *supra* note 23, at 1925; *see also* Pascale, *supra* note 9, at 340.

Furthermore, since most victims are women, deepfake pornography is a "form of collective discrimination and should be treated as such."[30] However, note that

> [t]he recognition that intimate activity and nudity can be viewed as discrediting and shameful—and result in discrimination—is not to suggest that intimate behaviors and nudity are discrediting and shameful. Intimate activities and naked bodies are not dirty. Because sexuality, gender, and the human body are central to identity formation and intimacy, we need the freedom to manage their boundaries.[31]

Additionally, unlike other forms of sexual harassment, deepfake pornography exclusively utilizes tools and information within the bounds of cyberspace. Professor Mary Anne Franks, a leading scholar on digital sexual privacy, articulated four features of cyberspace that intensify "the effects of unwilling online embodiment."[32] These features are: (1) anonymity, which allows harassers to attack without revealing their identity, making it challenging for victims to seek remedies; (2) amplification, where harassers can easily reach a large audience and even incite others to join in; (3) permanence, as online attacks are difficult to erase; and (4) virtual captivity or publicity, where the pervasive nature of cyberspace harassment means victims cannot easily escape its effects.[33] Unlike "real life" harassment, which may be confined to specific locations, online harassment can follow the victim everywhere, as attacks indexed by search engines are accessible to virtually anyone, including colleagues, classmates, clients, or family members, regardless of location.[34]

In conclusion, the devastating impact of deepfake pornography on women draws upon a morality-based justification for an urgently needed legal solution. Recognizing a legal violation for deepfakes under a sexual privacy and autonomy framework—the goal of the post-consent framework—must start with the recognition that deepfake pornography

---

30. *See* Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 260 n.118 (2011), https://journals.library.columbia.edu/index.php/cjgl/article/view/2621 (citing Catharine MacKinnon, *Directions in Sexual Harassment Law*, 31 NOVA L. REV. 225, 227 (2007)). Franks discusses "cyber harassment, which is closely tied to deepfake porn. *Id.* at 260.

31. *See* Citron, *supra* note 23, at 1898.

32. *See* Franks, *supra* note 30, at 255–56. Franks argues that these effects "are potentially even more pernicious and long-lasting than real-life harassment." *Id.*

33. *See id.*

34. *Id.*

operates as a form of discrimination and harassment that necessitates stronger legal protections.

II. LEGISLATIVE RESPONSES TO DEEPFAKE PORNOGRAPHY: GAPS AND SHORTCOMINGS

Several states have rushed to address the issue of deepfake pornography through new legislation.[35] Others apply existing laws related to nonconsensual pornography, child pornography,[36] election law,[37] and other offenses, to cases involving deepfakes. Within the states that have passed legislation specifically targeted to combat deepfake pornography, some create civil causes of action, a criminal statute, or both.[38] Among the states with criminal statutes outlawing deepfake pornography, "there is a high degree of variance in classification of crime, penalty, and even criminal prosecution."[39]

Even putting aside the issues posed by the lack of unanimity among state responses, state laws will fail to properly resolve deepfake pornography because "the internet has transcended the boundaries of state regulation."[40] Thus, a federal statute is the necessary authority to address deepfake pornography.[41] Several bills introduced in Congress, including the AI Labeling Act of 2023,[42] the DEFIANCE (Disrupt Explicit Forged Images

35. *See* Appendix; *see also* Claire Withycombe, *States Race to Restrict Deepfake Porn as It Becomes Easier to Create*, WASH. STATE STANDARD (Apr. 11, 2024), https://washingtonstatestandard.com/2024/04/11/states-race-to-restrict-deepfake-porn-as-it-becomes-easier-to-create/.

36. As of August 2025, five states and the territory of Washington, D.C. do not include AI or computer-generated images in their CSAM (child sexual abuse material, A.K.A. child pornography) statutes: Alaska, Colorado, Massachusetts, Ohio, Vermont, and Washington, D.C. *See State Laws Criminalizing AI-Generated or Computer-Edited Child Sexual Abuse Material (CSAM)*, ENOUGH ABUSE (Dec. 2024), https://enoughabuse.org/get-vocal/laws-by-state/state-laws-criminalizing-ai-generated-or-computer-edited-child-sexual-abuse-material-csam/.

37. Legislation on deepfakes in the election or political context are not included in the Appendix.

38. *See* Appendix, *infra*.

39. *See* Press Release, Office of Rep. María Elvira Salazar, *U.S. Senate Passes Salazar's Bill to Protect Deepfake Revenge Porn Victims*, (Dec. 21, 2023) https://salazar.house.gov/media/press-releases/us-senate-passes-salazars-bill-protect-deepfake-revenge-porn-victims ("The companion version to Reps. María Elvira Salazar (R-FL) and Madeleine Dean's (D-PA) bill."). *See also* Appendix, *infra*, for the variation in state law responses to criminalizing deepfake pornography.

40. 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, 265 (2024), https://www.americanbar.org/content/dam/aba/publications/Jurimetrics/spring-2024/real-people-in-fake-porn-how-a-federal-right-of-publicity-could-assist-in-the-regulation-of-deepfake-pornography.pdf.

41. *See* Delfino, *supra* note 11, at 927 (arguing that federal criminalization of pornographic deepfakes is necessary because the issue crosses jurisdictional boundaries and existing state-level efforts are too slow and inconsistent, and a national law would provide uniformity, greater resources for enforcement, and highlight the serious harm caused to victims).

42. *See* S. 2691, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/2691/text.

and Non-Consensual Edits) Act of 2024,[43] and the Preventing Deepfakes of Intimate Images Act,[44] have not been passed in both chambers. One such act, unanimously passed in the United States Senate in December 2024, is the TAKE IT DOWN Act (Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act).[45] The Act "protects victims of real and deepfake 'revenge pornography,'" which classifies both under the term nonconsensual intimate images ("NCII").[46] The Act has several features that align and reflect the underpinning of the post-consent framework:[47]

> The TAKE IT DOWN Act addresses these issues while protecting lawful speech by:
>
> • Criminalizing the publication of NCII or the threat to publish NCII in interstate commerce;
> • Protecting good faith efforts to assist victims by permitting the good faith disclosure of NCII for the purpose of law enforcement or medical treatment;
> • Requiring websites to take down NCII upon notice from the victims within 48 hours; and
> • Requiring that computer-generated NCII meet a 'reasonable person' test for appearing to realistically depict an individual, so as to conform to current First Amendment jurisprudence.[48]

The TAKE IT DOWN Act defines "consent" as "an affirmative, conscious, and voluntary authorization made by an individual free from force, fraud, duress, misrepresentation, or coercion."[49]

The Act would apply where the "publication of the intimate visual depiction (I) is intended to cause harm; or (II) causes harm, including psychological, financial, or reputational harm, to the identifiable

---

43. *See* S. 3696, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3696 (providing a civil right to action that "would apply both to existing law relating to nonconsensual disclosure of intimate images and the new cause of action for nonconsensual deepfake intimate images").

44. *See* H.R. 3106, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/3106?s=1&r=68.

45. H.R. 8989, 118th Cong. (2024), https://www.congress.gov/118/bills/hr8989/BILLS-118hr8989ih.pdf.; Salazar, *supra* note 39 ("The companion version to Reps. María Elvira Salazar (R-FL) and Madeleine Dean's (D-PA) bill.").

46. Salazar, *supra* note 39 ("The companion version to Reps. María Elvira Salazar (R-FL) and Madeleine Dean's (D-PA) bill.").

47. Analyzed in detail in Part IV, *infra*.

48. Salazar, *supra* note 39.

49. H.R. 8989 § (h)(1)(A).

individual."[50] This allows a court to find, in a circumstance where there was no consent, a defendant guilty even if they claim they did not have intent to cause harm to the victim, which has been a successful defense for revenge porn litigation in the past.[51]

Even so, these well-meaning legislative solutions continue to use consent as their linchpin. As a result, these statutes do not provide sufficient protection for future victims of deepfake pornography. Deepfake pornography fundamentally operates outside of the boundaries of traditional consent frameworks because victims are entirely unaware that their digital face or body is being used, manipulated, or distributed until later, and thus they usually never even receive the *opportunity* to consent or refuse.[52] However, the TAKE IT DOWN Act is the federal legislation closest to employing the post-consent framework; thus, it is analyzed throughout this Note.

III. POSTMODERN LEGAL THEORY AND CYBERFEMINISM – FOUNDATIONS FOR REDEFINING CONSENT IN DIGITAL SPACES

Postmodern legal theory and cyberfeminism serve as helpful foundations for creating a definition of legal autonomy that does not rest on conventional notions of consent. The consent paradigm assumes that autonomy only exists where an individual is given the opportunity to choose or refuse participation. But deepfake technology provides the ability to create sexually explicit content without *any* direct involvement or awareness on the part of the victim, which in turn would mean individuals do not have autonomy over themselves in the digital space. As such, the concept of consent fails to address the unique nature of deepfake technology and the consequences of harm existing in a digital space. Consent's rigid binaries do not straightforwardly apply on the internet, where digital identity is fluid. Even in the digital space, an individual's autonomy should be given the opportunity to be exercised.

---

50. *Id.* at (h)(2)(A)(iv) (citation modified).

51. *See* Citron, *supra* note 23, at 1933.

52. *See* Mark Dsouza, *Undermining Prima Facie Consent in the Criminal Law*, 33 LAW & PHIL. 489, 493 (2014), https://www.jstor.org/stable/24572523 ("As with any choice, in order for the chooser to truly have authorship over the choice, the choice must be hers, and not forced upon her by someone else.").

Postmodern legal theory, with its critique of rigid legal categories,[53] provides a valuable lens to understand the complexities of identity in the digital space. Postmodern thinkers challenge the idea of fixed identities and emphasize the fluid and fragmented nature of personhood.[54] This perspective is particularly useful for examining how deepfake technology complicates traditional legal categories like consent and autonomy in digital spaces.[55] By framing identity as fluid, postmodern theory allows for a more nuanced understanding of how deepfake pornography disrupts conventional legal concepts.[56]

Cyberfeminism also contributes significantly to discussions of consent and autonomy in digital spaces by examining how digital technologies, including the internet and artificial intelligence, shape gender and identity in ways that both empower and oppress individuals.[57] Cyberfeminism is

---

53. For a quick background, see *Modernism and Postmodernism in Jurisprudence: Exploring Perspectives and Implications*, MYJUDIX, https://www.myjudix.com/post/modernism-and-postmodernism-in-jurisprudence-exploring-perspectives-and-implications (last visited Jan. 26, 2025) ("Postmodernism emerged as a response to the limitations and assumptions of modernism. It rejects the idea of objective truth and challenges the notion of a single, universal narrative. In the context of jurisprudence, postmodernism questions the neutrality and objectivity of legal systems, emphasizing the role of language, power, and social context in shaping legal meaning.").

54. *See, e.g.*, Frederick J. White, *Personhood: An Essential Characteristic of the Human Species*, 80 *LINACRE Q.* 74 (2013), https://doi.org/10.1179/0024363912Z.00000000010; *see also* J. Meese et al., *Posthumous Personhood and the Affordances of Digital Media*, 20 MORTALITY 408 (2015), https://doi.org/10.1080/13576275.2015.1083724.

55. *See generally* Douglas Husak, *The Complete Guide to Consent to Sex: Alan Wertheimer's Consent to Sexual Relations*, 25 LAW & PHIL. 267 (2006). Consent is a concept with implications far beyond sexual offenses, as it can make otherwise wrongful behavior permissible. However, its ontological nature remains a subject of debate. Some view consent as a mental state, similar to belief or intention, while others see it as a behavioral act. A third perspective suggests consent is a hybrid of both mental state and behavior. The crucial aspect of consent lies not in its metaphysical definition, but in the conditions that grant it the power to transform impermissible actions into permissible ones. This transformative ability stems from its capacity to alter an individual's reasons for acting. Consent is not solely a philosophical problem; it has practical implications, particularly in the realm of sexual offenses. For instance, unexpressed consent, while potentially existing as a mental state, cannot effectively alter an individual's motivations. Further complicating the issue of consent are conditions that can render it invalid or ineffective. Deception, coercion, and incapacitation are widely recognized factors that can undermine consent, particularly in the context of sexual interactions.

56. *Cf.* Jonathan Herring, *Rape and the Definition of Consent*, 26(1) NATIONAL LAW SCHOOL OF INDIA REVIEW 62, 63 (2014), http://www.jstor.org/stable/44283782 ("In the context of rape, consent is required because a sexual penetration is a prima facie wrong. . . . The defendant needs to have a good reason for the sexual penetration. This can only be provided by consent.").

57. *See generally* Kira Hall, *Cyberfeminism*, in COMPUTER-MEDIATED COMMUNICATION (1996), https://www.colorado.edu/faculty/hall-kira/sites/default/files/attached-files/hall-1996-cyberfeminism.pdf. It is important to note that cyberfeminism is a diverse group of theories, discussions, and practices related to gender and digital culture, focusing on the empowerment of women through digital technology. It is not a unified concept but rather a collection of various theoretical and political stances related to technology and gender. For example, Hall describes how some cyberfeminists believe pornography online empowers women, while others (similar to the author of this Note) believe it contributes to female oppression online.

especially pertinent to deepfake pornography, which lies at the intersection of technology, gendered power dynamics, and violations of consent.

When cyberfeminism emerged in the early 1990s,[58] it was rooted in the idea that cyberspace could dismantle established binaries, especially gender binaries, by offering new forms of identity and embodiment.[59] However, this optimistic vision contrasts sharply with the ways digital spaces have since become sites of exploitation, particularly for women.[60] As one scholar notes, there is "a particularly poignant irony in the nonconsensual sexualized embodiment of women in cyberspace"—a space that was once envisioned as a realm of liberation.[61] Today, cyberfeminist perspectives vary: some argue that online spaces provide an escape from gender embodiment and its associated oppressions, while others contend that digital technologies only reinforce traditional gender hierarchies.[62] What remains clear is that cyberfeminism sheds light on how digital technologies often amplify existing power imbalances[63] and expose the limitations of traditional understandings of consent in addressing the ongoing nature of gendered cyber harassment.[64]

Postmodern legal theory and cyberfeminist insights guide the way to a new framework to address the ways deepfake pornography violates personhood in digital spaces. The postmodern and cyberfeminist critique of consent supports the argument that traditional legal frameworks are ill-suited to address the harms of deepfakes, and that a new legal model—one

---

58. *See* Franks, *supra* note 30, at 254; Hall, *supra* note 57, at n.3 (1996), https://www.colorado.edu/faculty/hall-kira/sites/default/files/attached-files/hall-1996-cyberfeminism.pdf.

59. *See* Franks, *supra* note 30, at 254; *see also* Trevor Scott Milford, *Revisiting Cyberfeminism: Theory as a Tool for Understanding Young Women's Experiences*, *in* EGIRLS, ECITIZENS 55 (Jane Bailey & Valerie Steeves ed. 2015), https://books.openedition.org/uop/492 ("Early cyberfeminists conceptualized cyberspaces as fundamentally liberating, theorizing their capacity to move beyond the traditional binaries and limitations of popular gender and feminist politics.").

60. *See* Franks, *supra* note 30, at 228 ("The volume and viciousness of cyber-attacks—especially sexualized attacks—on women by men suggests that cyberspace cannot be thought of as a place where, on balance, women and men can participate equally. Rather, it is a place where existing gender inequalities are amplified and entrenched.").

61. *Id* at 227.

62. Milford, *supra* note 59.

63. *See* Franks, *supra* note 30, at 228.

64. *Id.* at 238 ("The virtual world has not only reproduced the various forms of discrimination that exist in the physical world, but has allowed them to flourish in ways that would not be possible in the physical world."); *id.* at 226 ("Cyberspace idealism often produces conflicting accounts of the 'realness' of cyberspace. On the one hand, cyberspace is often regarded as more real than real life-that is, the ability to control the terms of representation makes cyberspace existence more genuine. On the other hand, harms committed in cyberspace are often dismissed as 'not really real,' as they are by their nature not physical, bodily harms. The way this tension plays out in terms of the law's recommended role in cyberspace can yield schizophrenic results: freedom of speech, for example, in cyberspace is 'really real' and must be vigorously protected; harassment in cyberspace is not 'really real' and thus should not be taken very seriously.").

that recognizes the fluidity of online identity while also recognizing that it exists in a space that continues gendered oppression—is essential.

IV. THE POST-CONSENT FRAMEWORK: A PROPOSED SOLUTION TO DEEPFAKE PORNOGRAPHY

The post-consent framework[65] moves beyond the traditional notion of consent, recognizing that, in the digital age, a single moment of permission is insufficient to protect individuals from the ongoing risks of identity appropriation and exploitation. Rather than a legislative proposal or a fully implementable policy, this framework is meant to serve as a conceptual lens for law and policymakers to use when crafting legal solutions to combat deepfake pornography.

At its core, this framework shifts the idea of consent to use one's digital identity from a one-time grant of consent paradigm to one acknowledging continuous control because digital identity is fluid, persistent, and vulnerable to misuse. Consent-based models fail to account for the complexities of online spaces because an individual's identity is no longer solely tied to their physical presence but extends into the digital space—the concept of *digital personhood*.[66] Digital personhood can be exploited without their subject's knowledge or approval, often in harmful ways, such as in the creation and dissemination of deepfake pornography. Since one's digital personhood is shaped by how they are represented, manipulated, and perceived online,[67] consenting to create a digital personhood does not guarantee continued autonomy of that personhood.

In light of this reality, the post-consent framework holds that individuals should maintain control over their digital personhood, even after they have posted an image online. By shifting the focus from consent to control, it better accounts for the ways digital identities can be manipulated and repurposed far beyond that the initial act of consent.

---

65. The "post-consent" term is created by the Author but was inspired by the term "postmodern" in postmodern legal theory, see Part III, *infra*, and cyberfeminism's "post-gender" ideal. *See* Milford, *supra* note 59, at 55 ("Early cyberfeminists conceptualized cyberspaces as fundamentally liberating, theorizing their capacity to move beyond the traditional binaries and limitations of popular gender and feminist politics. Human-machine mergers made possible by technology were imagined as facilitators of "post-gender worlds": and virtual spaces were initially envisioned as utopian sites of unrestricted, transcendent emancipation from gender-related constraints.").

66. Inspired by J. Meese et al., *Posthumous Personhood and the Affordances of Digital Media*, 20 MORTALITY 408 (2015), https://doi.org/10.1080/13576275.2015.1083724.

67. *See* Shanyang Zhao, *The Digital Self: Through the Looking Glass of Telecopresent Others*, 28(3) SYMBOLIC INTERACTION 387–405 (Summer 2005), https://www.jstor.org/stable/10.1525/si.2005.28.3.387.

A. The Four Principles of the Post-Consent Framework:

The theoretical underpinnings for the post-consent framework can be categorized into four principles, albeit with many overlapping concepts: (1) Digital Personhood and Identity Control, (2) Non-Material Harms and Psychological Integrity, (3) Shifting from Consent to Accountability, and (4) Autonomy as Control, Not Just Choice.

1. Digital Personhood and Identity Control

Under the post-consent framework, individuals should have a right to control the representation of their digital personhood. This includes a legal recognition of the distinctiveness of one's digital identity as an extension of their "real world" self. Current law generally treats digital representation as a mere intellectual property or defamation issues, an approach that is inadequate because civil causes of action force the victim to be the driving force of litigation and leave the perpetrators without criminal penalties.[68] Civil litigation also limits the victim's relief to economic damages, to which many perpetrators may be judgment-proof.[69] A post-consent framework would establish a right to digital integrity, where the unauthorized use of someone's likeness, even if digitally altered, would be treated as a direct violation of their digital personhood.[70]

This principle emphasizes that identity is not limited to physical or intellectual aspects but also includes a virtual dimension. Deepfakes exploit someone's digital personhood by distorting and manipulating the individual's image, causing real psychological, emotional, and reputational harms that are currently underappreciated by existing legal structures. The post-consent framework would recognize the fragmentation of identity caused by deepfakes as a distinct harm that warrants legal redress under criminal law.

---

68. For an analysis on why even though civil laws such as "defamation and obscenity laws seem like a logical fit, the very artifice of deepfake images will preclude most of these claims," see Pascale, *supra* note 9, at 345–50. *See also* Salazar, *supra* note 39 ("Bringing a civil action can be incredibly impractical. It is time-consuming, expensive, and may force victims to relive trauma.").

69. *Judgment-Proof*, LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/judgment-proof (last visited Sept. 9, 2025) ("The term judgment-proof or judgment proof is an adjective for persons against whom enforcing a judgment is not feasible, or not worth the costs of pursuing litigation. The term is used in situations where a plaintiff would be no better off with a favorable judgment than they would be had they chosen not to sue the defendant in the first place. In other words, people are judgment-proof if they lack the resources or insurance to pay a court judgment against them.").

70. Concept drawn from Citron, *supra* note 23, at 1898, and expanded to more areas.

2. Non-Material Harms and Psychological Integrity

Traditional legal frameworks often rely on tangible harm—financial, physical, or reputational—to justify legal action.[71] The post-consent framework recognizes that harm includes non-material harms, particularly psychological and emotional injuries. These harms should be addressed under criminal law, which routinely accommodates intangible harms that have typically been left out of civil law.[72]

The post-consent framework would create legal standards for assessing these non-material harms, ensuring that victims of deepfakes have avenues for compensation or remedy based on the emotional and psychological impact, rather than solely on reputational or economic damage. Deepfake pornography creates a legal wrong because it is a violation of the individual's sexual autonomy and digital identity and thus, a *rights-based* violation.

The language "rights-based violation" is adopted from a study on deepfake pornography (which the authors referred to as AI-Generated Non-Consensual Intimate Images ("AIG-NCII")) that was conducted to, in part, investigate the arguments for and against the unacceptability of deepfake pornography.[73] Based on the responses they heard from participants, the authors divided the arguments into two different broad classes.[74] Some participants "argued that creating AIG-NCII was acceptable as long as no harms manifested, e.g., 'It's not harming me or blackmailing me . . . [a]s long as it doesn't get shared I think it's ok.'"[75] They labeled this viewpoint a "harms-based analysis."[76] The other class of arguments came from participants who argued that AIG-NCII was "unacceptable, even if never shared, because it was a 'violation of my body'" and thus constituted what

71. *See Revenge Porn and Deep Fake Technology: The Latest Iteration of Online Abuse*, BU Law: Dome (Aug. 10, 2023), https://sites.bu.edu/dome/2023/08/10/revenge-porn-and-deep-fake-technology-the-latest-iteration-of-online-abuse/ ("[M]any revenge porn statutes [which are very similar, if not the same, statues which deepfake pornography is included under] include a "harm" requirement, which is difficult to prove and requires victims to expose even more of their private life in a public arena.").

72. *See* Ronald V. Miller, Jr., *When Can You Sue for Emotional Distress*, LAWSUIT INFORMATION CENTER, https://www.lawsuit-information-center.com/when-can-you-sue-for-emotional-distress.html (last visited Sept. 9, 2025) ("Tort law in the U.S. generally recognizes emotional distress (often referred to as 'pain & suffering') as a type of injury for which monetary damages can be awarded. In most states, however, damages can only be awarded for emotional distress if the emotional distress is directly caused by physical harm.").

73. *See* Natalie Grace Brigham et al., *"Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery* 11–12 (June 16, 2024), https://www.usenix.org/system/files/soups2024-brigham.pdf.

74. *Id.*

75. *Id.* at 7.

76. *Id.* at 12.

they deemed a "rights-based evaluation."[77] Regarding the study's terms, the post-consent framework aligns itself with the latter approach—arguing that deepfakes are a right-based violation, specifically sexual privacy[78] and digital identity rights.[79]

The TAKE IT DOWN Act addresses this by drafting the statute to encompass harm caused by such violations, including psychological, financial, or reputational harm to the individual affected.[80] This departs from the typical civil causes of action which typically requires a showing of an economic damages, even if characterized as an emotional harm.[81]

3. Shifting from Consent to Accountability

In the current legal landscape, consent is the linchpin for determining whether a violation has occurred in the context of privacy, sexual autonomy, or pornography. However, in cases of deepfake pornography, the question of consent is often moot because the victim is typically unaware until after the fact. The post-consent framework proposes a shift toward accountability, where the onus is placed on the creators, distributors, and platforms hosting deepfake content to ensure that the digital manipulation of individuals is lawful.

This would involve a stricter regulatory environment where digital platforms have a heightened duty to verify the authenticity of user-uploaded content and ensure that individuals featured in deepfakes have the ability to report and request the content be removed. This could translate into a duty of care for the online platform to remove the content reported unless the deepfake creator, as opposed to the victim, can prove they had permission. Failing to meet these standards would lead to increased liability for platforms, encouraging the development of better detection mechanisms and accountability measures for the misuse of deepfake technology.

4. Autonomy as Control, Not Just Choice

In a post-consent framework, autonomy is defined as the right to maintain control over one's identity, regardless of whether active choices are made in the moment. The law would focus on ongoing autonomy, where individuals have continuous control over their image and likeness in digital spaces. Legal remedies would be available not just for the initial violation, but for any subsequent use or distribution that perpetuates the harm, shifting

77. *Id.*
78. *See generally* Citron, *supra* note 23.
79. *See, e.g.*, Part II, *supra*, on a digital personhood.
80. *See* H.R. 8989 § 2(h)(2)(A)(iv)(II).
81. *See, e.g.*, table *infra* the Appendix. *See also* Miller, Jr., *supra* note 72.

the focus from isolated moments of consent, or lack thereof, to a broader, more fluid understanding of personal control over one's virtual representation. The TAKE IT DOWN Act accomplishes this by criminalizing creation, distribution, and threats to do either.

The TAKE IT DOWN Act defines an "identifiable individual" (or the victim) as the person "whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with such intimate visual depiction."[82] The Act allows for both the "face" and the "body" in deepfake pornography to be considered in the prosecution, epitomizing the post-consent framework.

B. Potential Criticisms of the Post-Consent Framework

There are several potential criticisms of the post-consent framework.[83] One anticipated criticism is the risk of legal overreach. Some may argue that granting individuals continuous control over their digital identity could lead to frivolous lawsuits or attempts to censor content that does not cause genuine harm.[84] However, this criticism is overstated as the post-consent framework is meant to be narrowly applied to address the specific harms caused by deepfake pornography, rather than to create overly broad restrictions on the use of images online.

Criticisms are also likely to focus on the practicality of implementing laws that grant individuals ongoing control over their digital identity. Defining and regulating what it means to have continuous control over one's likeness in digital spaces presents significant challenges given the decentralized and global nature of the internet. Additionally, enforcement across different jurisdictions would be difficult.[85] These challenges are significant but not impossible to overcome, if the directions in Part V are implemented.

Another potential criticism is that the post-consent framework could potentially infringe on freedom of speech and artistic expression by granting

---

82. *See* H.R. 8989 § 2(h)(1)(C).

83. This discussion is by no means meant to be exhaustive of the potential criticisms of the framework, but merely some selected points that warranted discussion in this Note. Additionally, The TAKE IT DOWN Act faces criticisms that are not discussed in this Note. *See, e.g.*, Joe Mullin, *The TAKE IT DOWN Act: A Flawed Attempt to Protect Victims That Will Lead to Censorship*, ELECTRONIC FRONTIER FOUNDATION ("EPP") (Feb. 11, 2025), https://www.eff.org/deeplinks/2025/02/take-it-down-act-flawed-attempt-protect-victims-will-lead-censorship.

84. *See, e.g.*, Mullin, *supra* note 83.

85. See Part V, Section D, *infra*, for discussion.

individuals broad control over their digital likenesses.[86] Repercussions could manifest in the censorship of satirical content, parodies, or other creative works that use manipulated images. However, there is extremely limited, and possibly nonexistent, use of deepfake pornography for these purposes. Nonetheless, possible solutions to this concern include adapting existing legal standards to determine when digital likeness use is legitimate expression or harmful exploitation.

V. RECOMMENDATIONS FOR IMPLEMENTING THE POST-CONSENT FRAMEWORK

Lawmakers must proactively address the issues posed by deepfake pornography for legal protections to keep pace with the technological advancements, especially since the harm is so unique and without legal redress, victims are left with nothing. Below are a few policy recommendations for how lawmakers can implement the post-consent framework.[87]

These recommendations include creating a criminal statute prohibiting the creation and distribution of deepfake pornography, establishing international enforcement mechanisms[88] such as international law enforcement, and leveraging technological advancements like "hashing and matching."[89] International legal bodies could collaborate to establish a clear definition of continuous control in the context of digital identity, which could be incorporated into national legislation and international agreements. A global collaborative body could also facilitate cross-border enforcement of digital identity rights.

---

86. First Amendment arguments no doubt arise and could complicate the application of the post-consent framework. For an articulation of "ways to consider First Amendment free speech concerns while also safeguarding victims of nonconsensual pornography, such as deepfakes," see Delfino, *supra* note 11, at 925–26. For an argument on how pornography in general should not be given First Amendment protection, see CATHARINE A. MACKINNON, ONLY WORDS 29, Harvard University Press 1993 ("At stake in constructing pornography as 'speech' is gaining constitutional protection for doing what pornography *does:* subordinating women through sex.").

87. As with the criticisms, this discussion is by no means exhaustive or considerate of all possibilities, but merely a demonstration of some initial ideas.

88. See Part V, Section D, *infra*, for discussion.

89. See note 103, *infra*, for information on hashing technology.

A. Criminalizing Creation, Possession, and Distribution of Deepfake Pornography

The post-consent framework advocates for the federal criminalization of deepfake pornography[90] as a distinct offense with its own penalties,[91] not precluding a private civil cause of action. In this sense, the TAKE IT DOWN Act gets close to implementing this aspect of the post-consent framework by making it a federal crime to use an interactive computer service to knowingly publish, or threaten to publish, non-consensual intimate imagery on online platforms.[92]The bill justified criminalizing the publication of deepfake pornography, as opposed to creating a civil cause of action, by noting that "bringing a civil action can be incredibly impractical. It is time-consuming, expensive, and may force victims to relive trauma."[93] Civil actions create no criminal history of the defendants' actions and cause the victim to be the driver of litigation. Furthermore, the criminal law theories of deterrence (punishing criminals to discourage future crime), retribution (punishing criminals to provide justice for the crime), and prevention (preventing crime by intervening before it occurs) all support criminalizing deepfake pornography.[94]

B. Deepfake Detection and Verification Requirements for Platforms

Beyond prosecuting individual perpetrators, we should require online platforms to create processes to identify and remove deepfake pornography. Holding platforms liable for failing to remove deepfake pornography would incentivize the development of more effective prevention technologies and the swift removal of reported content.

---

90. For an analysis on why even though civil laws such as "defamation and obscenity laws seem like a logical fit, the very artifice of deepfake images will preclude most of these claims," see Pascale, *supra* note 9, at 345–50.

91. Even though this Note advocates that deepfake pornography is a form of sexual harassment, it should not be included under existing sexual abuse or rape laws because such laws still rely on consent.

92. *See* H.R. 8989 §§ 2(h)(2)(A)–(B).

93. *See* Salazar, *supra* note 39.

94. *See* Mari Privette, *Theories of Punishment*, 29 U. KAN. CITY L. REV. 46 (1961).

The TAKE IT DOWN Act tackles platform liability in its third section, Notice and Removal of Nonconsensual Intimate Visual Depictions.[95] The section mandates that covered platforms have one year from the date of the act's enactment to create a process for individuals to report and request the removal of deepfakes on their platform(s).[96] In addition to establishing a reporting and removal process, the bill requires platforms to give "clear and conspicuous notice" of that process.[97] Upon receiving a valid removal request, the platform must remove the intimate visual depiction as soon as possible, within 48 hours of the request.[98] Additionally, they should try to identify and remove any known identical copies of the depiction.[99] This process would protect covered platforms from liability for actions taken in good faith to disable access to or remove material believed to be a nonconsensual intimate visual depiction, regardless of the depiction's ultimate legal status.[100]

In sum, the TAKE IT DOWN Act accomplishes the goal of incentivizing online platforms to establish a reporting system for victims to request removal of deepfake pornography on their platforms. However, the process requires the individual, or their authorized representative, to identify the depiction with enough information for the platform to locate it, declare a good faith belief that the depiction is non-consensual, along with supporting information, and provide contact information.[101] This requirement falls short of fully aligning with the post-consent framework's principles, as it effectively imposes a quasi-pleading standard on victims, forcing them to describe the deepfake and provide the basis of its non-consensual nature. This creates at least two major dangers: the continued victimization of the individual from online platforms employees having to review any reported content, and the discretion given to online platforms to determine if the reported content justifies removal.

The first issue is particularly significant under the post-consent framework, which prioritizes sexual privacy and digital autonomy.[102] The TAKE IT DOWN Act's proposed reporting process would necessitate a victim, who is looking to get the material removed, to subject the material to further review—causing further victimization. To mitigate this,

---

95. H.R. 8989 § 3(b)(1) (charging the Federal Trade Commission with enforcement of this section).

96. *Id.* at § 3(a)(1)(A).

97. *Id.* at § 3(a)(2).

98. *Id.* at § 3(a)(3). This is similar to data privacy laws such as Europe's "right to be forgotten." *See Right to Be Forgotten*, GDPR.EU, https://gdpr.eu/right-to-be-forgotten/ (last visited Oct. 5, 2024).

99. H.R. 8989 § 3(a)(3) (2024).

100. *Id.* at § 3(a)(4).

101. *See id.* at § 3(a)(1)(B)(i)– (iii).

102. *See* Part IV, *supra.*

legislation should mandate that platforms implement detection tools capable of identifying deepfakes without human review. One potential solution is leveraging "hash-value" technology[103]—already in use for child sexual abuse material—to index known deepfake pornography. This would allow platforms to verify deepfake content without requiring direct examination, thereby reducing exposure and minimizing harm.

The second issue arises from delegating decision-making power to the online platforms, effectively eliminating judicial oversight and depriving victims of due process protections.[104] The government is generally better positioned than private platforms to define and safeguard individual rights, as platforms may prioritize their own interests over the protection of those rights. Accordingly, the post-consent framework calls for government oversight to ensure a consistent and impartial process for victims seeking redress.

C. Digital Identity Rights Legislation

Beyond a federal criminal statute, implementing the post-consent framework calls for a change in privacy laws to address the realities of digital personhood.[105] Specifically, it argues that governments should enact specific laws that recognize digital identities as extensions of physical personhood, providing individuals with legal recourse when their virtual identities are manipulated or exploited without their permission.

Expanding the right of publicity in intellectual property law, for instance, could serve as the legal avenue for granting individuals the ability to control the commercial use of their likeness[106] in deepfakes.[107] The post-consent framework advances that a renewed right of publicity[108] should exist in tandem with a federal criminal statute. The digital identity right aspect of a right to publicity is not reflected in the TAKE IT DOWN Act, but the NO FAKES Act would "empower victims of deep fakes; safeguard human

---

103. For background on how "hashing and matching" works, see *What Is Hashing?*, CODEACADEMY BLOG (Mar. 27, 2025), https://www.codecademy.com/resources/blog/what-is-hashing/.

104. *See, e.g.*, U.S. CONST. amend. V. The Fifth Amendment Due Process Clause only applies to actions done by the federal government.

105. "Digital personhood" is being used in the same sense it was introduced in this Note at Part III, *supra*.

106. *Right of Publicity*, INT'L TRADEMARK ASS'N, https://www.inta.org/topics/right-of-publicity/ (last visited Oct. 7, 2024).

107. Such as proposed by Constantino, *supra* note 40, at 263 (arguing that "[i]n conjunction with federal legislation that gives victims a private right of action, the enactment of a broad federal right of publicity could provide an adequate avenue for victims to claim civil penalties").

108. *See id.*

creativity and artistic expression; and defend against sexually explicit deepfakes."[109]

D. Global Collaboration for Cross-Jurisdictional Enforcement

Even if the post-consent framework were perfectly reflected in a federal criminal statute in the United States (which would still render it subject to administration changes, litigation, and judicial review), the nature of both the crime and digital space it occurs within require recognition that deepfake pornography is a problem global in scale.[110]

Since deepfake pornography often involves global actors, international cooperation would be essential for enforcing post-consent protections. Collaborative efforts in law enforcement should be developed to address cross-border violations, allowing victims to seek remedies in multiple jurisdictions and holding perpetrators accountable across borders.

Regardless of the exact organizations investigating and enforcing the law, it is also important to establish a global victim-centered voice in the conversation. For example, The Reclaim Coalition to End Online Image-Based Sexual Violence is a global network that integrates survivor leadership into policy discussions worldwide,[111] which could offer a potential "global hub" for victims of deepfake pornography.

CONCLUSION

Deepfake pornography presents a unique challenge to existing legal frameworks and requires a jurisprudential shift to a post-consent model. Lawmakers, courts, and online platforms need to rethink the boundaries of consent in the digital age and adopt policies that focus on protecting individuals' autonomy and dignity by granting them ongoing control over their digital identity. This Note advocates for the use of a *post-consent framework*.

The post-consent framework reframes the legal discourse around deepfake pornography, moving away from the narrow lens of consent and toward a more comprehensive understanding of identity, autonomy, and accountability in the digital age. By addressing the unique harms posed by

---

109. *See* Salazar, *supra* note 39.

110. Aligning with other scholars who advocate for a global solution. *See, e.g.*, Haleluya Hadero, *Deepfake Porn Could be a Growing Problem Amid AI Race*, AP NEWS (Apr. 16, 2023, 10:24 a.m.), https://apnews.com/article/deepfake-porn-celebrities-dalle-stable-diffusion-midjourney-ai-e7935e9922cda82fbcfb1e1a88d9443a. ("[Noelle Martin,] an attorney and legal researcher at the University of Western Australia, says she believes the problem has to be controlled through some sort of global solution.").

111. *See* The Reclaim Coalition to End Online Image-Based Sexual Violence, PANORAMA GLOBAL, https://panoramaglobal.org/the-reclaim-coalition/.

deepfakes and empowering individuals to maintain control over their virtual identities, this approach offers a pathway toward more robust legal protections in a world where technology increasingly blurs the boundaries of reality and representation. In short, we need to adapt to the realities of the digital age. Deepfake pornography poses a new threat to personhood; it causes distinctly gendered harms, necessitating a distinct framework, global enforcement, and victim advocacy efforts.

APPENDIX

Table of enacted state legislation criminalizing nonconsensual deepfake pornography, not limited to minors.

State	Citation	Summary
Alabama	Ala. Code § 13A-6-240	Provides that a person commits the crime of creating a private image if he or she knowingly creates, records, or alters a private image when the depicted individual has not consented to the creation, recording, or alteration and the depicted individual had a reasonable expectation of privacy; provides for criminal penalties for violations; provides that no developer or provider of technology shall be held in violation solely for providing or developing technology used by another person.
California	Cal. Civ. Code § 1708.86 (West)	Gives individuals a cause of action against anyone who creates, discloses, or facilitates the creation of sexually explicit deepfake material depicting them without consent, including material depicting minors. The law treats operators of deepfake pornography services as presumed to have knowledge of nonconsent and requires them to stop providing

		services when notified. Exceptions include disclosures for law enforcement, legal proceedings, public interest, or protected speech. Victims can recover economic, noneconomic, and statutory damages, while public prosecutors can also bring civil actions. Internet service providers are generally not liable for merely transmitting or hosting third-party content.
Colorado	Colo. Legis. Serv. Ch. 402 (S.B. 24-011) (West)	Criminalizing posting a private image for harassment if the actor posts or distributes through the use of social media or any website any photograph, video, or other image displaying the real or simulated (including digitally created or altered) private intimate parts of an identified or identifiable person eighteen years of age or older or an image displaying sexual acts of an identified or identifiable person.
Florida	Fla. Stat. Ann. § 836.14 (West)	Criminalizing possession of any image depicting an identifiable person engaged in sexual conduct, or any image that has been created, altered, adapted, or

		modified by electronic, mechanical, or other means, to portray an identifiable person engaged in sexual conduct.
Georgia	Ga. Code Ann. § 16-11-90 (West)	Criminalizing the posting of an image or video, including falsely created ones, which depicts nudity or sexuality of a person, and is harassment or cause loss to the person.
Hawaii	Haw. Rev. Stat. Ann. § 711-1110.9 (West)	Criminal offense for deepfakes, with intentional creation, disclosure, or threat to disclose any image or video of any "composite fictitious person" that includes "recognizable physical characteristics of a known person" without consent of depicted person and with intent to harm substantially that person in multiple respects, or revenge.
Idaho	Idaho Code Ann. § 18-6606 (West)	Criminal offense for a knowing disclosure of explicit synthetic material with knowledge or reason to know that identifiable person in deepfake did not consent to the disclosure and disclosure would cause person substantial emotional distress. Also, an offense to disclose same with intent to annoy, terrify, threaten, intimidate,

		harass, offend, humiliate, or degrade an identifiable person portrayed in whole or in part in the explicit synthetic media
Illinois	720 Ill. Comp. Stat. Ann. 5/11-23.7	Criminalizes the non-consensual dissemination of sexually explicit digitized depictions, including deepfakes. It defines "sexually explicit digitized depiction" as any image, photograph, film, video, digital recording, or other depiction that has been created, altered, or otherwise modified to realistically depict intimate parts or sexual activity in which the depicted individual did not engage
Indiana	Ind. Code Ann. § 35-45-4-8 (West)	Provides that certain images created by artificial intelligence or similar means constitute an "intimate image" for the crime of distributing an intimate image. Specifies that an intimate image, for purposes of the criminal offense, must appear to depict the alleged victim.
Iowa	Iowa Code Ann. § 708.7 (West)	Criminalizing anyone who disseminates, publishes, distributes, posts, or causes to be disseminated, published, distributed, or posted a visual depiction of

		another person in a state of partial or full nudity or engaging in a sex act. "Another person" includes an individual, recognizable by the person's face, likeness, or other distinguishing features.
Louisiana	La. Stat. Ann. § 14:73.13	Criminalizing the knowing creation, possession, or distribution of a sexual deepfake that realistically depicts a person engaged in sexual conduct—without consent if the person depicted is an adult, or regardless of consent if the person depicted is a minor. "Deepfake" does not include any material that constitutes a work of political, public interest, or newsworthy value, including commentary, criticism, satire, or parody, or that includes content, context, or a clear disclosure visible throughout the duration of the recording that would cause a reasonable person to understand that the audio or visual media is not a record of a real event.
Minnesota	Minn. Stat. Ann. §§ 604.32, 617.262 (West)	Criminal offense and private cause of action for knowing dissemination of deepfakes depicting intimate parts or sexual acts without consent.

New Hampshire	N.H. Rev. Stat. Ann. §§ 507:8-j, 638:26-a	Criminal felony and private cause of action for all deepfakes, with knowing creation, distribution, or presentation, made for a variety of purposes such as harassment or embarrassment.
New York	N.Y. Penal Law § 245.15 (McKinney)	Criminalizing the dissemination or publication of an intimate image with intent to cause harm, where the image has any intimate parts exposed or are engaged in sexual conduct, including any image created or altered by digitization, where the person can be identified from the image or information in the image.
Oregon	O.R.S. § 163.472	Criminalizing the unlawful dissemination of an intimate image of a person, including digital images, for a person that knowingly discloses an image of another person whose intimate parts are visible or who is engaged in sexual conduct if a reasonable person would be harassed, humiliated, or injured by the disclosure, and without their consent.
South Dakota	S.D. Codified Laws § 22-21-4	Criminalizing the knowing, intentional dissemination of any image of another person

		that includes deepfake images that depict the person in either a nude or partial nude state or a sexual act without that person's consent and with the intent to self-gratify or to harm the person in a variety of ways including embarrassment
Texas	Tex. Penal Code § 21.165	A person commits an offense if, without the effective consent of the person appearing to be depicted, the person knowingly produces or distributes by electronic means a deepfake video that appears to depict the person with the person's intimate parts exposed or engaged in sexual conduct.
Utah	Utah Code Ann. § 76-5b-203 (West)	Criminalizing the knowing distribution, duplication, or copying of an intimate image of an adult without their consent, under circumstances in which the individual depicted in the image has a reasonable expectation of privacy (with some specialized exceptions). The person depicted must actually suffer emotional distress or harm as a result.
Vermont	Vt. Stat. Ann. tit. 13, § 2606 (West)	Criminalizing knowing disclose a nude or sexually explicit image of an identifiable person

		without their consent, that would cause a reasonable person to suffer harm, with penalties of up to two years in prison or a $2,000 fine, and up to five years or a $10,000 fine if done for financial gain. It also prohibits websites and online services from charging fees to remove such images and allows victims to sue for damages and seek court orders to stop further distribution.
Virginia	Va. Code Ann. § 18.2-386.2 (West)	Provides, for the purposes of the prohibition against the unlawful dissemination or sale of certain images of another person, that "another person" includes a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic.
Washington	Wash. Rev. Code Ann. § 9A.86.010 (West)	A person commits the crime of disclosing intimate images (including a deepfake) when the person knowingly shares an intimate image of another

		person that the person knows or should have known was without consent, and with reason to know that disclosure would cause harm.