IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Consent, Deepfakes & Revenge Porn: Confronting Non-Consensual Intimate Content

Ekata Deb, PG Scholar, LLM-Criminology, Reva University, Bengaluru, KA, India

Abstract: The increase of AI-enabled deepfakes along with its widespread dissemination of intimate images without consent, an act of revenge porn has seen to blur the boundaries of digital accord, undermining personal autonomy and privacy. This paper examines the legal, technological, and ethical dimensions of non-consensual intimate image (NCII), drawing on interdisciplinary paradigms and legislative developments across key jurisdictions. Drawing insights from the U.S. TAKE IT DOWN Act, Virginia's Deep Fake Pornography Law, and India's legislative lacuna—this study highlights enforcement challenges and technological limitations. This paper recommends harmonized legislation, mandatory platform mitigation, victim-centric redressal mechanisms, along with initiatives for digital literacy to fortify digital consent in an era of synthetic media.

Keywords: Digital Consent; Deepfakes; Revenge Porn; Non-Consensual Intimate Image (NCII); Cyber Law; Artificial Intelligence; Online Privacy; Platform Regulation

Introduction

In traditional digital consent practices, individuals must agree to share intimate content explicitly[1]. Still, modern artificial intelligence technology allows wrongdoers to make fake pornographic content with unsuspecting subjects, thus undermining the concept of informed consent[2]. Authentic intimate images that spread against victims will continue to circulate known as "revenge porn", despite legal difficulties which prevent content removal from online platforms[3]. Victims of Deepfake technology face legal challenges because many jurisdictions have passed revenge porn laws but these statutes do not protect victims whose intimate content was created using AI.[4] The detection of synthetic nature of intimate content remains slower than the development of creation technologies, leading to difficulties in taking down content by international law enforcement.[5]

The classic meaning of digital consent requires direct and affirmative consent for sharing intimate photos.[6] Modern AI technologies enable malicious users to generate authentic pornographic material from unsuspecting materials through advanced capabilities while opposing current concepts of liberty and consent.[7] Genuine intimate images continue to spread without authorization throughout the Internet under the term "revenge porn."[8] Victims face dual obstacles when attempting to remove their content online because they

[1] "Understanding 'Consent' under the Digital Personal Data Protection Act, 2023 (DPDPA)" (CISO Platform, December 30, 2024) <https://www.cisoplatform.com/profiles/blogs/understanding-consent-under-the-digital-personal-data-protection->.

[2] Humans For Ai, "Hidden Dangers of AI: Deepfake Technology - Humans for AI - Medium" *Medium* (November 16, 2024) <https://medium.com/@humansforai/hidden-dangers-of-ai-deepfake-technology-a0a940951dc2>.

[3] Alaattinoğlu D, "Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps" (2022) 30 Feminist Legal Studies 157 <https://doi.org/10.1007/s10691-021-09486-y>

[4] Ibid

[5] Ibid 1-2

[6] "Consent for Sharing Photos and Videos | eSafety Commissioner" (*eSafety Commissioner*) <https://www.esafety.gov.au/young-people/consent-sharing-photos-videos>.

[7] King TC and others, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" (2019) 26 Science and Engineering Ethics 89 <https://doi.org/10.1007/s11948-018-00081-0>

[8] Iman Said and Rachel L McNealey, "Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration" (2022) 38 Journal of Interpersonal Violence 5430 <https://doi.org/10.1177/08862605221122834>.

must deal with social discrimination and elaborate legal processes.[9] Deepfake pornography victims cannot obtain legal protection through revenge porn laws because jurisdictions explicitly state that AI-generated content falls outside their legal boundaries.[10] The rapid development of deepfake technology surpasses the progress in detecting synthetic intimate content, resulting in synthetic materials becoming increasingly difficult to recognize and remove.[11] Digital content spreads rapidly across different borders, creating problems for transnational enforcement due to the technological lag, which makes content removal challenging.[12]

The laws protecting non-consensual intimate image (NCII) provide limited protection against the current difficulties that deepfake technology generates.[13] Technological companies must execute and collaborate with the "Take It Down Act"[14] for its enforcement to succeed, although the U.S. Senate approved the bill unanimously. The Online Safety Act 2023[15] is a significant United Kingdom legislative measure to fight online dangers, including NCII. The Online Safety Act 2023 faces scrutiny because the effectiveness and capability of its implementation procedures to regulate AI-generated content remains unclear.[16]

The technological detection of deepfake materials presents significant difficulties to systems.[17] Fast-evolving deepfake generation technologies currently exceed the capabilities of developers' AI detection tools to identify them. Platforms, together with law enforcement agencies, find it hard to swiftly detect and delete malicious content because of the difference in capabilities, which extends the amount of time victims need to endure psychological trauma.[18]

Digital Consent Theory

According to Danielle Citron and Robert Chesney, synthetic media has destroyed traditional authenticity standards, which leads to a new definition of consent as a process that continues contextually instead of one singular action[19]. Adopting digital consent models should adapt to AI development while adding a feature for users to revoke and affirmatively give their permissions through built-in platform framework systems.[20] The field of digital consent now examines consent as a sustained process because it needs to adjust according to the development of AI technologies combined with platform changes.[21] The findings from Chesney and Citron indicate that synthetic media breaks authentication processes and eliminates conventional consent requirements. They also reveal how click-through agreements cause numerous digital consent problems, according to Richards and Hartzog[22], through their “pathologies” concept. Protection of consent within digital spaces now adopts dynamic framework systems based on biomedical ethics explicitly developed for these domains to enable platform administrators to control user permissions.[23] The Synthetic Media Framework of the Partnership on AI[24] presents a set of “3C” (consent, control, collaboration) principles that serve as criteria to develop protections relating to the individual rights in computational systems. The experts suggest that user consent remains valid when people actively engage with platforms through “transparent choice architectures” to prevent frequent system changes.[25]

The authors Danielle Citron and Robert Chesney state that deepfake technology removes elements that require informed consent authorization. The authors create a model for evaluating consent that expands

---

[9] ibid
[10] Equality Now, “Viewing Consent through a Digital Lens - Equality Now” (*Equality Now*, September 18, 2024) <https://equalitynow.org/news_and_insights/viewing-consent-through-a-digital-lens/>.
[11] ibid
[12] Eleanor Bird and others, “The Ethics of Artificial Intelligence: Issues and Initiatives” (2020) report PE 634.452 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf>.
[13] Ibid 2-11
[14] S.4569 — 118th Congress (2023-2024)
[15] 2023 c. 50
[16] Peter Coe, “Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and Its Disconnection from Free Speech Law and Theory*” (2023) 15 Journal of Media Law 213 <https://doi.org/10.1080/17577632.2024.2316360>.
[17] ibid
[18] ibid
[19] Danielle K Citron and Robert Chesney, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” (*Scholarly Commons at Boston University School of Law*) <https://scholarship.law.bu.edu/faculty_scholarship/640/>.
[20] “The Impact of AI on Consent Management Practices” (*https://secureprivacy.ai/*, April 19, 2025) <https://secureprivacy.ai/blog/ai-consent-management>.
[21] Ibid-16
[22] Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461 (2019). Available at: https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11
[23] Ibid 2-22
[24] “PAI’s Responsible Practices for Synthetic Media” (*Partnership on AI - Synthetic Media*, March 19, 2025) <https://syntheticmedia.partnershiponai.org/#:~:text=A%20Framework%20for&text=Partnership%20on%20AI's%20(PAI)%20Responsible,generated%20or%20modified%20by%20AI.>.
[25] ibid

beyond basic authorization permissions to multiple dimensions.[26] In their research paper "Pathologies of Digital Consent," Neil Richards and Woodrow Hartzog state that standard "I agree" agreements lead to pathological effects because users expect different terms than platforms deliver.[27] The research by Leon Trakman et al. studied digital consent development while distinguishing moral consent that transfers obligations and rights from legal, enforceable consent, and identifying the areas of AI exploitation and the related weaknesses.[28]

A review in BMC Medical Ethics demonstrates that dynamic consent introduces adaptable, longitudinal permission based on medical ethics, allowing users to modify throughout time. Yet, these tools show limited deployment beyond clinical settings. The Synthetic Media Framework of Partnership on AI requires users to have revocable permissions through layered consent interfaces (the "3Cs"), which allow them to modify their consent status after AI content generation. Complementing these, ACM research on policy-based consent management outlines a four-layer service architecture for automated, domain-agnostic consent enforcement, bridging regulatory compliance with user control.

"Transparent choice architectures" leverage UI design to clarify consent implications, avoiding dark-pattern nudges that undermine user autonomy. AI businesses advocate treating consent as an ongoing dialogue—regularly re-engaging users when new data uses or features arise and making opt-in/opt-out settings accessible in plain language. Nevertheless, geographies lag in adopting digital provenance standards (e.g., watermarking, metadata tags) for AI media, impairing source verification and consent auditing.[29]

Revenge Porn and Legal Gaps

State-level revenge porn laws in the U.S. provide some avenues for criminalization, yet they predominantly target the distribution of authentic images and rarely anticipate AI-mediated alterations[30]. Scholars recommend elevating image-based sexual abuse to the same status as physical sexual offenses, decoupling prosecution from obscenity or defamation paradigms[31]. Revenge-porn statutes in the United States now cover almost every state. Still, they focus on real images and often require proof of intent to harm, leaving AI-generated content unaddressed[32]. Federal law (Violence Against Women Act, VAWA 2022) provides a private right of action for victims of non-consensual image distribution, yet omits explicit reference to deepfakes.[33] Scholars urge elevating image-based sexual abuse to the level of physical sexual offenses—decoupling it from obscenity or defamation frameworks—and highlight severe mental health impacts on survivors[34]. On the technological side, AI-driven detection tools exist (e.g. Deep Fake-o-meter), but performance degrades on compressed or high-fidelity forgeries, and platform integration remains uneven.[35] This paper examined U.S. legal frameworks, scholarly reform proposals, technological hurdles, and journals mostly leading the debate on nonconsensual intimate image (NCII)[36].

State-Level Legislation in the U.S.: As of 2024, 48 states, the District of Columbia, and Guam have enacted laws criminalizing the nonconsensual distribution of intimate images, typically requiring that the photos depict nudity or sexual activity and that the distributor intends to harass or harm the victim[37]. Penalties range from misdemeanors (up to one year in jail or fines under $2,500)[38] to felonies (multi-year sentences and fines up to $150,000)[39], depending on state statutes. However, these laws uniformly target authentic images

---

[26] Ibid 3-19
[27] Ibid 3-22
[28] Leon Trakman, Robert Walters and Bruno Zeller, "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience" (2020) 29 Information & Communications Technology Law 218 <https://doi.org/10.1080/13600834.2020.1726021>.
[29] *Proceedings of International Conference on Generative AI, Cryptography and Predictive Analytics* (2025) <https://doi.org/10.1007/978-981-97-9132-3>.
[30] Rebecca A Delfino, "Pornographic Deepfakes: The Case For Federal Criminalization Of Revenge Porn's Next Tragic Act," vol 88 (2019) <https://fordhamlawreview.org/wp-content/uploads/2019/12/Delfino_December_A_2.pdf>.
[31] ibid
[32] ibid
[33] "Fact Sheet: Reauthorization of the Violence Against Women Act (VAWA) | The White House" <https://perma.cc/SL2R-NZRX>.
[34] Nicola Henry and Gemma Beard, "Image-Based Sexual Abuse Perpetration: A Scoping Review" (2024) 25 Trauma Violence & Abuse 3981 <https://doi.org/10.1177/15248380241266137>.
[35] "DeepFake-o-Meter v2.0: An Open Platform for Deepfake Detection" (*IEEE Conference Publication | IEEE Xplore*, August 7, 2024) <https://ieeexplore.ieee.org/document/10707802/>.
[36] Maria Noemi Paradiso, Luca Rollè and Tommaso Trombetta, "Image-Based Sexual Abuse Associated Factors: A Systematic Review" (2023) 39 Journal of Family Violence 931 <https://pmc.ncbi.nlm.nih.gov/articles/PMC10126554/>.
[37] Ibid 2-8
[38] "§ 18.2-11. Punishment for Conviction of Misdemeanor" <https://law.lis.virginia.gov/vacode/title18.2/chapter1/section18.2-11/>.
[39] Reporters Committee for Freedom of the Press, "Criminal Penalties Archives" (*The Reporters Committee for Freedom of the Press*) <https://www.rcfp.org/reporters-recording-sections/criminal-penalties/>.

and rarely contemplate AI-mediated alterations, leaving victims of deepfake pornography without statutory recourse.[40] At the federal level, the Violence Against Women Act Reauthorization Act of 2022 created a private civil cause of action for individuals whose intimate images are disclosed without consent.[41] Still, it does not explicitly include AI-generated content within its definition of "sexually explicit visual depictions". Moreover, Section 230 of the Communications Decency Act, 1996 protects platforms from liability for user-generated content, complicating enforcement and takedown efforts across state lines.[42]

Scholarly Calls for Reclassification and Reform: Multiple academic sources maintain that revenge porn needs to be seen as sexual violence instead of a privacy or property violation[43]. According to McGlynn et al. 2020, image-based sexual abuse results in severe psychological damage, which includes depression, anxiety, and suicidal thoughts; therefore, they argue for equal penal procedures.[44] The existing statutes uphold patriarchal standards through their emphasis on ex-partner motives while neglecting victims' bodily control thus recommending courts to establish non-consensual distribution as a form of criminal rape.[45] The initial consensual sharing creates obstacles for legal remedies; therefore, they propose that NCII offenses should exist independently from obscenity or defamation law.[46] Global statutory frameworks identifies key removal mechanisms and legislative lacunae that hinder victim redressal.[47]

Technological Challenges in Detection and Enforcement: AI-driven detection tools—such as the University of Buffalo's Deep Fake-o-meter—apply machine-learning classifiers to flag synthetic media, yet accuracy plummets for high-quality deepfakes and compressed video.[48] Recent advances in proactive forensics (watermarks, blockchain provenance, ensemble detection) show promise but are not widely deployed on major platforms.[49] Digital media forensics surveys underscore that most detectible algorithms require high computational resources and human verification, limiting scalability for platforms that must process millions of uploads daily.[50] Moreover, heterogeneous international standards for media authentication further impede cross-border cooperation in takedowns and prosecutions.[51]

Deepfakes and Synthetic Media

Advances in Generative Adversarial Networks (GANs) have accelerated the fine-tuning of deepfake pornography, with platform traffic to deepfake sites growing from under 2,000 videos in 2018 to over 13,000 by 2022.[52] Political discourse around deepfakes underscores broader societal risks, but scant attention has been paid to intimate-image misuse, which disproportionately harms women and marginalized groups.[53] Deepfake pornography now represents about 98% of all deepfake videos online, overwhelmingly targeting women (99% of victims) and amplifying gendered harms already endemic in revenge-porn contexts.[54] Though political deepfakes garner public attention for misinformation risks, sexualized synthetic media inflicts profound privacy, reputational, and psychological damage, especially on women in the public eye, such as

---

[40] Asher Flynn and others, "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse" (2021) 62 The British Journal of Criminology 1341 <https://lens.monash.edu/@politics-society/2024/04/18/1386624/legal-loopholes-dont-help-victims-of-sexualised-deepfakes-abuse>.

[41] "The Violence Against Women Act Reauthorization Act of 2022: Overview of Applicability to HUD Programs" (*Federal Register*, January 4, 2023) <https://www.federalregister.gov/documents/2023/01/04/2022-28073/the-violence-against-women-act-reauthorization-act-of-2022-overview-of-applicability-to-hud-programs>.

[42] Howard A Davidson and others, *Child Pornography and Prostitution: Background and Legal Analysis* (1987) <https://www.ojp.gov/pdffiles1/Digitization/109927NCJRS.pdf>.

[43] Ibid.

[44] Clare McGlynn and others, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2020) 30 Social & Legal Studies 541 <https://doi.org/10.1177/0964663920947791>.

[45] "Rehabilitating Compassionate Release: An 'Extraordinary and Compelling' Case for Increased Judicial Discretion" (*FLASH: The Fordham Law Archive of Scholarship and History*) <https://ir.lawnet.fordham.edu/ulj/vol52/iss4/4/>.

[46] Lawrence J. Fox, THE END OF PARTNERSHIP, 33 Fordham Urb. L.J. 245 (2005). Available at: https://ir.lawnet.fordham.edu/ulj/vol33/iss1/4

[47] Katarina Schwarz and Jing Geng, "Reasserting Agency: Procedural Justice, Victim-Centricity, and the Right to Remedy for Survivors of Slavery and Related Exploitation" (University of Nottingham and others, 2018) <https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/academic-publications/2019/march/schwarz-reasserting-agency.pdf>.

[48] ibid

[49] ibid

[50] ibid

[51] "UB's DeepFake-o-Meter Democratizes Deepfake Detection" (*University at Buffalo*, September 10, 2024) <https://www.buffalo.edu/news/releases/2024/09/ub-deepfake-o-meter-democratizes-deepfake-detection.html>.

[52] Tianxiang Shen and others, "Deep Fakes Using Generative Adversarial Networks (GAN)" <http://noiselab.ucsd.edu/ECE228_2018/Reports/Report16.pdf>.

[53] Mariëtte Van Huijstee and others, "Tackling Deepfakes in European Policy" (2021) report PE 690.039 <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf>.

[54] Ibid7-46

one-in-six U.S. Congresswomen recently found to be targeted by AI-generated explicit deepfakes.[55] Academics warn that marginalized racial and socioeconomic groups may face compounded vulnerability, as lower-quality source footage from affordable cameras is more easily manipulated and harder to authenticate in court.[56]

Technological Growth of Deepfake Pornography: Generative adversarial networks (GANs) underpin today's most convincing deepfake algorithms, pitting generator and discriminator networks against each other to refine synthetic outputs to near-photo realism.[57] Comprehensive mapping of the "deepfake landscape" underscores that nearly all deepfake content on mainstream social media is pornographic, yet platform moderation and provenance tagging remain rudimentary.[58]

Societal and Gendered Impacts: Deepfake pornography disproportionately harms women, 99% of victims, exploiting gendered power imbalances and contributing to technology-facilitated gender-based violence.[59] Public figures are especially vulnerable: a recent study found one-in-six U.S. Congress women targeted by explicit AI-generated videos, risking reputational damage and chilling effects on political participation.[60] Marginalized communities, often represented through lower-quality footage, may face skepticism in legal proceedings as courts demand high-tech verification for admissibility, perpetuating digital inequities.[61]

Detection Technologies and Forensic Challenges: State-of-the-art detection systems—such as the University of Buffalo's Deep Fake-o-meter—employ convolutional neural networks to flag synthetic artifacts, yet accuracy falls below 70% on compressed or high-resolution forgeries, and model robustness degrades under adversarial attacks.[62] Recent systematic reviews outline ensemble-based forensics (combining watermarking, blockchain provenance, and multiple detectors), but note that computational demands hinder real-time platform deployment.[63] A new survey of detection frameworks highlights generalization gaps: models trained on one dataset often fail on unseen forgeries, underscoring the need for larger, more diverse training corpora and standardized benchmarking. Meanwhile, emergent low-resource algorithms aim to decentralize detection to end-user devices, but remain experimental and untested at scale.[64]

Discussion

The analyzed cases demonstrate ongoing law enforcement challenges that emerge because technology advances beyond existing legal clarification methods. Harmful content continues to spread because reactive take-down systems do not react fast enough before it reaches multiple users, thus causing more trauma to victims and hurting trust in online environments. Mainstream platforms need to better integrate the provenance tools based on blockchain technology and the watermark technology to enhance their functionality.[65] The circulation of NCII material violates ethical standards by upholding gendered violence patterns, and experts from feminist theory advocate placing victim autonomy and dignity at the core of platform development.

Legal definitions have struggled to keep pace with rapidly evolving deepfake technologies, resulting in significant enforcement gaps; reactive takedown regimes not only fail to prevent proliferation of harmful content. Often retraumatize survivors; promising technological tool like digital watermarks and blockchain provenance remain sparsely deployed on mainstream platforms; and the circulation of non-consensual intimate image (NCII) perpetuates gender-based violence, prompting feminist scholars to call for centering victims' autonomy and dignity in both policy and design.

Numerous jurisdictions maintained their legal frameworks before the deepfake technology explosion, so they do not contain sufficient language to address AI-created intimate content, thus creating enforcement gaps because technologically advanced forgeries fail to match the definitions of "image-based abuse" in

---

[55] Chapman, Emily, "Unveiling the Threat- AI and Deepfakes' Impact on Women" (2024). Student Research Submissions. 567. https://scholar.umw.edu/student_research/567

[56] Vandinika Shukla, "Deepfakes and Elections: The Risk to Women's Political Participation" (*Tech Policy Press*, February 29, 2024) <https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/>.

[57] Ibid

[58] ibid

[59] Professor Clare McGlynn and Rüya Tuna Toparlak, "The New Voyeurism: Criminalising the Creation Of" (July 14, 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4894256>.

[60] Ibid 7-55

[61] ibid

[62] Fabian Bäumer and others, "Terrapin Attack: Breaking {SSH} Channel Integrity by Sequence Number Manipulation" (*USENIX*, November 20, 2024) <https://www.usenix.org/conference/usenixsecurity24/technical-sessions>.

[63] ibid

[64] ibid

[65] Amna Qureshi and David Megías Jiménez, "Blockchain-Based Multimedia Content Protection: Review and Open Challenges" (2020) 11 Applied Sciences 1 <https://www.mdpi.com/2076-3417/11/1/1>.

statutes.[66] The majority of state and federal proposed laws aim to punish the distribution of genuine photos or videos. Yet, deepfake creators face minimal prosecution risks under existing legislation. The U.S. lacks federal laws to prosecute deepfake porn creators so states have enacted varying and ineffective statutes to combat this form of abuse[67].

Current takedown regimes are predominantly reactive: platforms remove content only after victims file complaints, by that time, the material has often been widely shared and mirrored. Scholars document that these repeated reporting and verification cycles can retraumatize victims, echoing findings that interactions with justice systems usually intensify original harms and impede psychological recovery[68]. The reliance on notice-and-takedown also allows bad actors to exploit procedural delays, uploading altered or re-encoded files faster than moderators can identify and remove them[69].

Emerging provenance tools—such as Digimarc's media-watermarking combined with Numbers Protocol's blockchain tracking—offer robust methods to embed immutable creation metadata into digital assets, potentially verifying authenticity and consent status during uploading of the same[70]. However, integrating these systems into major social platforms remains minimal: few sites support metadata-preserving uploads, and most user workflows strip or ignore embedded provenance tags[71]. Moreover, standards for watermarking schemes are not harmonized, impeding cross-platform interoperability and limiting the scalability of blockchain-based verification[72].

The dissemination of NCII disproportionately targets women and other marginalized groups, reinforcing existing power imbalances and digital gendered violence.[73] Feminist theorists argue that policies must move beyond mere content removal and embed victim autonomy at every stage, allowing survivors to dictate how their data is used, shared, or archived.[74] Centering victims' dignity in platform design requires consent architectures that are revocable, transparent, and rooted in the lived experiences of those most harmed by NCII. This shift towards a trauma-informed approach aligns with calls to treat NCII as a form of sexual violence rather than a property or defamation issue, ensuring policies which address the relational and psychological dimensions of harm[75].

Recommendations

Before diving into the detailed recommendations, here is a high-level summary of our proposals: first, legislators must adopt clear, technology-neutral definitions of non-consensual intimate image (NCII) domestically and through international treaties[76]; second, platforms should face mandatory deployment of AI-driven detection tools and strict notice-and-takedown deadlines backed by meaningful penalties; third, victims need expedited digital grievance channels and pro bono legal clinics that integrate psychological support; fourth, digital literacy curricula must include modules on synthetic-media risks and affirmative digital consent; and finally, the adoption of standardized digital-provenance frameworks—such as watermarking and blockchain tags—must be incentivized across platforms.[77]

The law should establish a technology-independent definition of NCII, which includes real and AI-made images to stop deepfake makers from finding ways around the law. The bipartisan TAKE IT DOWN Act provides a foundation for national statutes because it criminalizes unauthorized sharing of intimate content, including deepfakes, while allowing the FTC to enforce unfair practices under the FTC Act[78]. International States should endorse and modernize the Budapest Convention by including explicit provisions to address NCII and strengthen cooperation for investigation support and evidence exchange[79]. The Council

---

[66] United States Copyright Office, "Copyright and Artificial Intelligence: Part 1 - Digital Replicas" (2024) <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf>.
[67] Greggwirth, "Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat - Thomson Reuters Institute" (*Thomson Reuters Institute*, June 27, 2024) <https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/>.
[68] Jill C. Engle, Sexual Violence, Intangible Harm, and the Promise of Transformative Remedies, 79 Wash. & Lee L. Rev. 1045 (2022).
[69] ibid
[70] ibid
[71] ibid
[72] Ibid 6-82
[73] Ibid 5-36
[74] Ibid 9-65
[75] American College Health Association. (2024). Addressing sexual and relationship violence: A trauma-informed approach. Silver Spring, MD: American College Health Association.
[76] Ibid 8-55
[77] ibid
[78] "FTC Proposes New Protections to Combat AI Impersonation of Individuals" (*Federal Trade Commission*, March 4, 2025) <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>.
[79] ibid

of Europe has already established nonconsensual image dissemination as a form of cyberviolence under its broader cybercrime and Istanbul frameworks, which provide standardized definitions.[80]

Social media platforms and hosting services must implement AI detection tools in their moderation systems based on the DOJ guidelines that establish new ethical standards for AI system deployment.[81] Social media platforms must meet the 24-hour deadline specified by the UK Code of Practice for online social media platforms when handling takedown requests, while setting specific content removal timelines.[82] The United Kingdom's Online Safety Act allows Ofcom to issue substantial fines to non-compliant services, which UK regulators, including the FTC, should adopt. The TAKE IT DOWN Act press release reveals platform cooperation needs through Senators Bill Cassidy, Ted Cruz, and Amy Klobuchar, who emphasize binding corporate duties.[83]

A digital grievance portal similar to Boston University's Center for Trauma & Mental Health must be established to process NCII complaints efficiently while providing emotional support for each case from start to finish.[84] The legal system needs financial support to develop free NCII clinic programs, including BU Law's experiential learning pro bono services, which provide specialized legal assistance without cost to victims.[85] A standardized operational model for crime victim clinics exists according to the National Institute of Justice, which offers maximum benefits to clients and applies to NCII situations. The redress program must provide immediate access to psychological support through legal processes to assist victims in dealing with the traumatic consequences caused by numerous appeals to take down content.

According to Equality Now recommendations, educational institutions should teach students about deepfakes through risk modules, showing them their detection methods while reinforcing digital consent education[86]. Public awareness programs demonstrate that organized curricula enhance critical thinking abilities, so they should extend their educational scope to teach about intimate content. Teachers must have access to the digital skills curriculum to develop their professional skills in consent, privacy education, and ethical media usage[87].

Auditing platforms must integrate watermark technology with blockchain-based verification systems to validate consented media files during their initial creation process.[88] The Data Trails partnership of Digimarc's keeps digital watermarks invisible during deepfake occurrences because these watermarks maintain an unchangeable link to the original metadata[89]. User trust and interoperability need the C2PA standard (Coalition for Content Provenance and Authenticity) to become mandatory for implementation by platforms and regulators, since it enables consent metadata embedding. Blockchain networks should integrate C2PA tags with additional consent data according to recommendations from ITU[90] and NIST[91] to establish tamper-evident provenance records[92].

Conclusion

The current situation shows that current laws and technological capabilities fail to adequately protect the intricate relationship between electronic consent and deepfake technology when used for revenge porn.

---

[80] "Texts Adopted - Combating Gender-Based Violence: Cyberviolence - Tuesday, 14 December 2021" (© *European Union, 2021 - Source: European Parliament*) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0489_EN.html>.

[81] Michael Abramov, "Ethical Considerations in AI Model Development | Keymakr" (*Keymakr*, February 20, 2025) <https://keymakr.com/blog/ethical-considerations-in-ai-model-development/>.

[82] Secretary of State for Digital, Culture, Media and Sport, "Code of Practice for Online Social Media Platforms" <https://assets.publishing.service.gov.uk/media/605e57a5d3bf7f717f35b8e0/Social_Media_Code_of_Practice_Easy_Read_V2.pdf>.

[83] Ted Cruz and others, "The TAKE IT DOWN Act" <https://www.young.senate.gov/wp-content/uploads/1-pager_TAKE-IT-DOWN-Act_6.18.2024-FINAL.pdf>.

[84] Abdul-Fatawu Abdulai and others, "Trauma-Informed Care in Digital Health Technologies: Protocol for a Scoping Review" (2023) 12 JMIR Research Protocols e46842 <https://pmc.ncbi.nlm.nih.gov/articles/PMC10337410/>.

[85] Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, "Strengthening Forensic Science in the United States: A Path Forward" (National Research Council 2009) <https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf>.

[86] ibid

[87] Christiane Annemann, Claudia Menge and Julia Gerick, "Teachers' Participation in Digitalization-Related Professional Development: An International Comparison" (2025) 15 Education Sciences 486 <https://www.mdpi.com/2227-7102/15/4/486>.

[88] Alsehli Abrar, Wadood Abdul and Sanaa Ghouzali, "Secure Image Authentication Using Watermarking and Blockchain" (2021) 28 Intelligent Automation & Soft Computing 577 <https://www.techscience.com/iasc/v28n2/42060/html>.

[89] "Digimarc and DataTrails Partner to Solve the Industry's Biggest Content Protection Challenge with Advanced Digital Watermarks and Cryptography" (April 10, 2024) <https://www.digimarc.com/press-releases/2024/04/10/digimarc-and-datatrails-partner-solve-industrys-biggest-content>.

[90] International Telecommunication Network

[91] National Institute of Standards and Technology

[92] "Overview - C2PA" <https://c2pa.org/>.

The public needs urgent protection for their rights and dignity through legal standards, including AI-generated and authentic NCII, innovative detection methods, and comprehensive victim support systems. Combining initiatives amongst lawmakers, technology companies, and civil society organizations is crucial to establishing a safer and more respectful digital environment.

The combination of digital consent with deepfake technology along with revenge porn generates a daunting environment with non-consensual intimate content that exceeds current legal and technological regulatory capabilities. A statutory framework that avoids technology dependency must be established immediately to prosecute AI-generated forgery cases because current legal loopholes allow these forged materials to escape prosecution. The deepfake offense concept proposed by Rebecca Delfino serves as a model for creating standardized domestic laws across the country, and international guidelines from the Council of Europe under Convention 108+ and the Budapest Convention define protocols to fight cyber violence across borders.

Advanced detection technologies must shift from experimental prototypes to ubiquitous platform features: GAO analyses show that current deepfake-forensic tools require more extensive, more diverse datasets and standardized benchmarks to reach reliable performance, and recent ITU-sponsored standards workshops emphasize multi-stakeholder collaboration on AI watermarking and media-authenticity protocols to embed provenance at scale.

Robust victim-support structures are equally essential. Free tools like StopNCII.org demonstrate the effectiveness of victim-centric case creation and hash-based takedown requests. Audit studies reveal that reporting via DMCA[93] mechanisms yield 100 percent removal within 25 hours, compared to zero percent under nonconsensual nudity policies, underscoring the need for unified reporting channels across platforms. The establishment of pro bono NCII legal clinics, together with integrated psychological counseling services, should receive funding from public-private partnerships to lower access barriers and minimize traumatic experiences.

Preventive measures hinge on widespread education and stakeholder alignment. The Axios forum of policymakers and experts from platforms and mental health fields confirmed that research-driven cooperative approaches, legislative changes, technical safety measures, and community involvement represent the best path to tackle the issue. The American Bar Association shows that safeguarding children and vulnerable populations needs joint sector participation since individual organizations cannot solve this problem.

The audit of dynamic consent systems with continuous context-based and revokable consents needs to create specific legislative measures to reach a 90 percent speed of removing real and synthetic NCII materials. The RSF works to secure international agreements that define deepfakes as threats to truthful information rights affecting both sexual violence cases and damage to reputation. The endorsement of Princeton-based legal scholars creates governmental reforms for AI development that protect democratic principles.

References

1. "§ 18.2-11. Punishment for Conviction of Misdemeanour" <https://law.lis.virginia.gov/vacode/title18.2/chapter1/section18.2-11/>
2. "Consent for Sharing Photos and Videos | eSafety Commissioner" (eSafety Commissioner) <https://www.esafety.gov.au/young-people/consent-sharing-photos-videos>
3. "DeepFake-o-Meter v2.0: An Open Platform for DeepFake Detection" (IEEE Conference Publication | IEEE Xplore, August 7, 2024) <https://ieeexplore.ieee.org/document/10707802/>
4. "Digimarc's and Data Trails Partner to Solve the Industry's Biggest Content Protection Challenge with Advanced Digital Watermarks and Cryptography" (April 10, 2024) <https://www.digimarc.com/press-releases/2024/04/10/digimarc-and-datatrails-partner-solve-industrys-biggest-content>
5. "Fact Sheet: Reauthorization of the Violence Against Women Act (VAWA) | The White House" <https://perma.cc/SL2R-NZRX>
6. "FTC Proposes New Protections to Combat AI Impersonation of Individuals" (Federal Trade Commission, March 4, 2025) <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>
7. "Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration" (2022) 38 Journal of Interpersonal Violence 5430 <https://pmc.ncbi.nlm.nih.gov/articles/PMC9969486/>
8. "Overview - C2PA" <https://c2pa.org/>

[93] Digital Millennium Copyright Act (DMCA) of 1998

9. "PAI's Responsible Practices for Synthetic Media" (Partnership on AI - Synthetic Media, March 19, 2025) <https://syntheticmedia.partnershiponai.org/#:~:text=A%20Framework%20for&text=Partnership%20on%20AI's%20(PAI)%20Responsible,generated%20or%20modified%20by%20AI.>

10. "Reasserting Agency: Procedural Justice, Victim-Centricity, and the Right to Remedy for Survivors of Slavery and Related Exploitation" (University of Nottingham and others, 2018) <https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/academic-publications/2019/march/schwarz-reasserting-agency.pdf>

11. "Rehabilitating Compassionate Release: An 'Extraordinary and Compelling' Case for Increased Judicial Discretion" (FLASH: The Fordham Law Archive of Scholarship and History) <https://ir.lawnet.fordham.edu/ulj/vol52/iss4/4/>

12. "Texts Adopted - Combating Gender-Based Violence: Cyberviolence - Tuesday, 14 December 2021" (© European Union, 2021 - Source: European Parliament) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0489_EN.html>

13. "The Impact of AI on Consent Management Practices" (https://secureprivacy.ai/, April 19, 2025) <https://secureprivacy.ai/blog/ai-consent-management>

14. "The Violence Against Women Act Reauthorization Act of 2022: Overview of Applicability to HUD Programs" (Federal Register, January 4, 2023) <https://www.federalregister.gov/documents/2023/01/04/2022-28073/the-violence-against-women-act-reauthorization-act-of-2022-overview-of-applicability-to-hud-programs>

15. "UB's DeepFake-o-Meter Democratizes Deepfake Detection" (University at Buffalo, September 10, 2024) <https://www.buffalo.edu/news/releases/2024/09/ub-deepfake-o-meter-democratizes-deepfake-detection.html>

16. "Understanding 'Consent' under the Digital Personal Data Protection Act, 2023 (DPDPA)" (CISO Platform, December 30, 2024) <https://www.cisoplatform.com/profiles/blogs/understanding-consent-under-the-digital-personal-data-protection->

17. Abdulai A-F and others, "Trauma-Informed Care in Digital Health Technologies: Protocol for a Scoping Review" (2023) 12 JMIR Research Protocols e46842 <https://pmc.ncbi.nlm.nih.gov/articles/PMC10337410/>

18. Abramov M, "Ethical Considerations in AI Model Development | Keymakr" (Keymakr, February 20, 2025) <https://keymakr.com/blog/ethical-considerations-in-ai-model-development/>

19. Abrar A, Abdul W and Ghouzali S, "Secure Image Authentication Using Watermarking and Blockchain" (2021) 28 Intelligent Automation & Soft Computing 577 <https://www.techscience.com/iasc/v28n2/42060/html>

20. Ai HF, "Hidden Dangers of AI: Deepfake Technology - Humans for AI - Medium" Medium (November 16, 2024) <https://medium.com/@humansforai/hidden-dangers-of-ai-deepfake-technology-a0a940951dc2>

21. Alaattinoğlu D, "Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps" (2022) 30 Feminist Legal Studies 157 <https://doi.org/10.1007/s10691-021-09486-y>

22. Annemann C, Menge C and Gerick J, "Teachers' Participation in Digitalization-Related Professional Development: An International Comparison" (2025) 15 Education Sciences 486 <https://www.mdpi.com/2227-7102/15/4/486>

23. Bäumer F and others, "Terrapin Attack: Breaking {SSH} Channel Integrity by Sequence Number Manipulation" (USENIX, November 20, 2024) <https://www.usenix.org/conference/usenixsecurity24/technical-sessions>

24. Bird E and others, "The Ethics of Artificial Intelligence: Issues and Initiatives" (2020) report PE 634.452 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf>

25. Citron DK and Chesney R, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (Scholarly Commons at Boston University School of Law) <https://scholarship.law.bu.edu/faculty_scholarship/640/>

26. Coe P, "Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and Its Disconnection from Free Speech Law and Theory*" (2023) 15 Journal of Media Law 213 <https://doi.org/10.1080/17577632.2024.2316360>

27. Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, "Strengthening Forensic Science in the United States: A Path Forward" (National Research Council 2009) <https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf>

28. Cruz T and others, "The TAKE IT DOWN Act" <https://www.young.senate.gov/wp-content/uploads/1-pager_TAKE-IT-DOWN-Act_6.18.2024-FINAL.pdf>

29. Davidson HA and others, Child Pornography and Prostitution: Background and Legal Analysis (1987) <https://www.ojp.gov/pdffiles1/Digitization/109927NCJRS.pdf>

30. Delfino RA, "PORNOGRAPHIC DEEPFAKES: THE CASE FOR FEDERAL CRIMINALIZATION OF REVENGE PORN'S NEXT TRAGIC ACT," vol 88 (2019) <https://fordhamlawreview.org/wp-content/uploads/2019/12/Delfino_December_A_2.pdf>

31. Equality Now, "Viewing Consent through a Digital Lens - Equality Now" (Equality Now, September 18, 2024) <https://equalitynow.org/news_and_insights/viewing-consent-through-a-digital-lens/>

32. Flynn A and others, "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse" (2021) 62 The British Journal of Criminology 1341 <https://lens.monash.edu/@politics-society/2024/04/18/1386624/legal-loopholes-dont-help-victims-of-sexualised-deepfakes-abuse>

33. Greggwirth, "Deepfakes: Federal and State Regulation Aims to Curb a Growing Threat - Thomson Reuters Institute" (Thomson Reuters Institute, June 27, 2024) <https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/>

34. Henry N and Beard G, "Image-Based Sexual Abuse Perpetration: A Scoping Review" (2024) 25 Trauma Violence & Abuse 3981 <https://doi.org/10.1177/15248380241266137>

35. JusCorpus, "LEGAL CHALLENGES OF DEEPFAKE TECHNOLOGY AND AI-GENERATED CONTENT IN INDIA - Jus Corpus" (Jus Corpus, April 20, 2025) <https://www.juscorpus.com/legal-challenges-of-deepfake-technology-and-ai-generated-content-in-india/>

36. King TC and others, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions" (2019) 26 Science and Engineering Ethics 89 <https://doi.org/10.1007/s11948-018-00081-0>

37. McGlynn C and others, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2020) 30 Social & Legal Studies 541 <https://doi.org/10.1177/0964663920947791>

38. McGlynn PC and Toparlak RT, "The New Voyeurism: Criminalising the Creation Of" (July 14, 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4894256>

39. Paradiso MN, Rollè L and Trombetta T, "Image-Based Sexual Abuse Associated Factors: A Systematic Review" (2023) 39 Journal of Family Violence 931 <https://pmc.ncbi.nlm.nih.gov/articles/PMC10126554/>

40. Proceedings of International Conference on Generative AI, Cryptography and Predictive Analytics (2025) <https://doi.org/10.1007/978-981-97-9132-3>

41. Qureshi A and Jiménez DM, "Blockchain-Based Multimedia Content Protection: Review and Open Challenges" (2020) 11 Applied Sciences 1 <https://www.mdpi.com/2076-3417/11/1/1>

42. Reporters Committee for Freedom of the Press, "Criminal Penalties Archives" (The Reporters Committee for Freedom of the Press) <https://www.rcfp.org/reporters-recording-sections/criminal-penalties/>

43. Said I and McNealey RL, "Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration" (2022) 38 Journal of Interpersonal Violence 5430 <https://doi.org/10.1177/08862605221122834>

44. Schwarz K and Geng J, "Reasserting Agency: Procedural Justice, Victim-Centricity, and the Right to Remedy for Survivors of Slavery and Related Exploitation" (University of Nottingham and others, 2018) <https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/academic-publications/2019/march/schwarz-reasserting-agency.pdf>

45. Secretary of State for Digital, Culture, Media and Sport, "Code of Practice for Online Social Media Platforms" <https://assets.publishing.service.gov.uk/media/605e57a5d3bf7f717f35b8e0/Social_Media_Code_of_Practice_Easy_Read_V2.pdf>

46. Shen T and others, "Deep Fakes Using Generative Adversarial Networks (GAN)" <http://noiselab.ucsd.edu/ECE228_2018/Reports/Report16.pdf>

47. Shukla V, "Deepfakes and Elections: The Risk to Women's Political Participation" (Tech Policy Press, February 29, 2024) <https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/>

48. Trakman L, Walters R and Zeller B, "Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience" (2020) 29 Information & Communications Technology Law 218 <https://doi.org/10.1080/13600834.2020.1726021>

49. United States Copyright Office, “Copyright and Artificial Intelligence: Part 1 - Digital Replicas” (2024) <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf>

50. Van Huijstee M and others, “Tackling Deepfakes in European Policy” (2021) report PE 690.039 <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf>