

SYMPOSIUM CONTRIBUTION

Nonconsensual Distribution of an Intimate Image and Artificial Intelligence: Approaches to Criminalization

Kayla Lemmon*

Abstract

The advancement of generative artificial intelligence (GAI) has expanded technology-facilitated sexual abuse, including the nonconsensual distribution of intimate images (NDII), into K–12 educational settings. This article examines the gaps in United States (U.S.) law governing AI-generated NDII through the lens of Indiana law and compares the U.S. approach with emerging European Union frameworks. Current U.S. laws remain largely reactive, relying on victim reporting and post-incident remedies while failing to meaningfully regulate the platforms and tools that facilitate synthetic NDII. This article argues that effective NDII prevention requires two central reforms: (1) clear and uniform statutory definitions and (2) upstream regulation of the platforms and tools that enable NDII generation and distribution. Drawing on the European Union’s regulatory approach, this article proposes a federal framework incorporating platform-level safeguards: age verification, consent verification, and watermarking requirements, while using K–12 digital literacy education as a complementary prevention measure. This article argues that together, these reforms would close enforcement gaps and provide more consistent protections for victims across the United States.

Keywords: EU law; nonconsensual distribution of intimate images; NDII; nonconsensual intimate images; NCII; generative artificial intelligence; artificial intelligence; deepfakes; synthetic NDII; technology-facilitated sexual abuse; platform accountability; upstream regulation; K–12 education; Indiana law; European Union Artificial Intelligence Act; TAKE IT DOWN Act

A Introduction

The rapid advancement of generative artificial intelligence (GAI) has dramatically expanded the scope, speed and anonymity of nonconsensual distribution of intimate images (NDII), leading to a surge in technology-facilitated sexual abuse and a pattern of harm that extends into K-12 educational settings. Existing legal frameworks at the federal and state levels in the United States of America (the ‘United States’), including recent acts such as the Tools to Address Known Exploitation by

* Kayla Lemmon, Juris Doctorate Candidate, Indiana Robert H. McKinney School of Law.

Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act) and Indiana Code § 35-45-4-8, illustrate efforts to counter authentic and AI-generated NDII (synthetic NDII). Yet, critical gaps remain.

This article argues that the United States' current approach requires two central reforms: (1) clear and uniform statutory definitions and (2) upstream regulation of the platforms and tools that allow users to generate NDII. Comparative frameworks from the European Union, such as the European Union Artificial Intelligence Act (Regulation 2024/1689) and the Violence Against Women Directive (2024/1385), illustrate how a federal approach to resolving these gaps could be structured.

In June 2025, the National Center for Missing and Exploited Children (NCMEC) released its first report on GAI-related child sexual exploitation.¹ Between 1 January and 30 June 2025, the organization received more than 440,000 reports of AI-generated child sexual abuse imagery, an astonishing surge from only 6,835 reports during the same period in 2024.² This growth underscores an alarming truth: advances in artificial intelligence have dramatically expanded the reach, speed and anonymity of technology-facilitated sexual abuse. The broader digital landscape mirrors this trend. In 2023, 98% of deepfake videos online were pornographic, and 99% of the individuals depicted were women.³ These figures reveal a gendered and systemic pattern of harm that has now reached K-12 environments, where approximately 15% of students report awareness of AI-generated or authentic intimate images of classmates.⁴

Intimate images, whether depictions or real images, destabilize victims because “the privacy of those victims is violated and the victims lose control over their likeness and identity”.⁵ Victims often struggle with hopelessness because they “may not be able to determine who has created the content” and therefore cannot determine how to prevent further incidents.⁶ Victims can experience depression, anxiety, suicidal ideation, fear of being in public, loss of trust, isolation and the “silencing effect” where “victims withdraw from online spaces and public discourse to avoid further abuse”.⁷

International approaches, particularly those emerging from the European Union, demonstrate how definitional clarity and upstream platform accountability,

1 Patricia Davis, *Spike in Online Crimes Against Children a “Wake-up Call”*, Nt'l Ctr. for Missing & Exploited Child (4 September 2025), <https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call> [https://perma.cc/4ECP-M9PF].

2 *Id.*

3 2023 *State of Deepfakes*, Security Hero (2023), <https://www.securityhero.io/state-of-deepfakes/#overview-of-current-state> [https://perma.cc/R7B7-PHUS].

4 Jasmine Mithani, *Kids Are Making Deepfakes of Each Other, and Laws Aren't Keeping Up*, The Markup (2 July 2025), <https://themarkup.org/artificial-intelligence/2025/07/02/kids-are-making-deep-fakes-of-each-other-and-laws-arent-keeping-up> [https://perma.cc/YXR3-R5AV].

5 DEFIANCE Act, S. 3696, 118th Congr. (2024).

6 *Id.*

7 *Id.*

complemented by K-12 educational interventions, could be operationalized at the federal level in the United States.

This article examines the intersection of NDII and GAI through the lens of Indiana law, situating it within broader federal and international developments. Ultimately, this article contends that effective NDII prevention and enforcement require two central reforms: (1) clear and uniform statutory definitions and (2) platform accountability through upstream regulation of the tools and platforms that enable NDII generation and distribution.

I. Background Information

1. Term Breakdown

The *Oxford Dictionary* defines Generative Artificial Intelligence (GAI) as “artificial intelligence designed to produce output, especially text or images, normally requiring human intelligence, typically by applying machine learning techniques to large collections of data”.⁸ This article utilizes the Federal Bureau of Investigation’s (FBI) definition of AI, as it discusses the consequences associated with unlawful AI use. The FBI defines AI as

Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight or that can learn from experience and improve performance when exposed to data sets; an artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; an artificial system designed to think or act like a human, including cognitive architectures and neural networks; a set of techniques, including machine learning (ML), that is designed to approximate a cognitive task; an artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.⁹

NDII occurs “when someone takes or shares an intimate image or video of you without your permission”.¹⁰ NDII goes by many names, the most common of which are “image-based sexual abuse”, “nonconsensual pornography” or “revenge porn”.¹¹ Synthetic NDII, known as “deepfakes”, is a variation of NDII that refers to “the

8 *Generative AI*, Oxford Dictionary, https://www.oed.com/dictionary/generative-ai_n?tab=fact-sheet#1411915320 [<https://perma.cc/V5YS-JUW6>] (last accessed 16 November 2025).

9 Artificial Intelligence, Federal Bureau of Investigation, <https://www.fbi.gov/investigate/counter-intelligence/emerging-and-advanced-technology/artificial-intelligence> (last accessed 16 November 2025).

10 *What Is the Nonconsensual Distribution of Intimate Images?*, Fed. Trade Comm’n: Consumer Advice, <https://consumer.ftc.gov/node/77453> [<https://perma.cc/6ZXU-A2NU>] (last accessed 28 October 2025).

11 *Id.*

creation and distribution of nonconsensual manipulated intimate material”.¹² This includes content

that is produced or distributed without the consent of the subject and has been altered potentially with artificial intelligence, to show nonconsensual intimate or explicit consent as ‘nonconsensual manipulated intimate material’.¹³

Deepfakes and other varieties of NDII can be in various forms, including imagery, video, audio and more.¹⁴ This article uses NDII as its primary term throughout, consistent with broader academic usage. Federal statutes in this article use nonconsensual intimate images (NCII).¹⁵ This interchangeability itself highlights the definitional inconsistency that this article identifies as one of the central issues requiring reform.

NDII is often used for sextortion, which is a “threat to distribute an individual’s real or synthetic intimate material without that person’s consent if the person does not comply with certain demands”.¹⁶ Perpetrators attempt to coerce the victim to pay money, send more images, perform sexual acts or take other actions against the victim’s wishes or interests.¹⁷ Regardless of whether the victim complies, perpetrators typically release the material.¹⁸ With technological advancements allowing perpetrators to create NDII, “victims struggle to prove the content is fake and to remove it from the internet, exacerbating the psychological and emotional toll”.¹⁹

2. *Impact on Victims*

Victims of NDII frequently experience severe and lasting psychological, financial and social harm.²⁰ NDII can impact “self-esteem, humiliation, depression, and anxiety” as well as other emotions and expressions.²¹ In a study conducted by the *Journal of Interpersonal Violence*, researchers identified five primary consequences of NDII: “fears of going out in public, engaging in relationships, applying to jobs and

12 *Image-Based Sexual Abuse Laws: Combat Nonconsensual AI Deepfakes*, RAINN (9 October 2025), <https://rainn.org/rainns-recommendations-for-legislators/image-based-sexual-abuse-laws-combat-nonconsensual-ai-deepfakes/> [https://perma.cc/8ML5-2EWY].

13 *Id.*

14 *Id.*

15 *Model Non-Consensual Intimate Imagery (NCII) Policy for K-12 Schools*, Ctr. for Democracy & Tech. (July 2025), <https://cdt.org/wp-content/uploads/2025/06/CDT-Model-NCII-Policy-Final.pdf> [https://perma.cc/Q7R8-GHQM].

16 *Frequently Asked Questions*, Cyber C.R. Initiative, <https://cybercivilrights.org/faqs/#terminology> [https://perma.cc/WY7G-3PQL] (last accessed 28 October 2025).

17 *Id.*

18 *How We Can Help You: Sextortion*, Federal Bureau of Investigations, <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sexortion> (last accessed 28 October 2025).

19 *Impact of Artificial Intelligence on Criminal and Illicit Activities*, Public-Private Analytic Exchange Program (2024), https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf [https://perma.cc/K7GC-E8QF] (2024).

20 Ana Murça et al., *Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women*, Nt’l Inst. of Health (June 2023), <https://pmc.ncbi.nlm.nih.gov/articles/PMC10239214/> [https://perma.cc/MXK3-PVAE].

21 *Id.*

seeking help, as well as an increase in depression and anxiety”.²² In each case examined by the study, the perpetrator was someone the victim knew, whether it was a former or current partner or a friend or an acquaintance.²³

Another important question to consider is how culture and the expectations society has for morality and conduct impact the regulation and reporting of NDII. Cultural norms frequently contribute to victim blaming, when others believe the victim is responsible (or partially responsible) for the crime occurring, and self-blame, which can occur when the victim believes they are responsible (or partially responsible) for the perpetrator’s actions.²⁴ Victims who create the material themselves are more likely to be blamed and to blame themselves, and those lacking experience with sexting are more likely to blame the victim.²⁵

NDII can also result in financial consequences, with many victims losing their jobs or having difficulty obtaining a job because the images appear online when the employer looks up the victim.²⁶ These emotions, judgments and financial consequences can occur when the victim was willing to send photos to the perpetrator, the perpetrator obtained them through other means or the perpetrator led the victim to believe they had intimate images.²⁷

3. *Escalation of NDII Through Technological Advancement*

As technology and social media evolve, NDII has become more accessible to perpetrators because they can act more “anonymously, instantaneously, and constantly”.²⁸ Along with social media, AI platforms and tool providers contribute greatly to the increasing NDII rates. Around 80% of GAI sites enable image generation, 42% allow video generation and a wide range allow content alteration, which “allows for facial changes, body changes, and the removal of clothing”.²⁹ AI-based nudification applications can take a clothed image of a person and produce nude images of them and do not require the consent of the person in the image.³⁰ Face-swap technology enables “the production of videos that are highly realistic and depict human actions that have never occurred” and “allows users to modify ... appearance, movement of

22 Jillian McKoy, *The Social Consequences of Nonconsensual Pornography*, Boston Univ. Sch. of Pub. Health (24 November 2020), <https://www.bu.edu/sph/news/articles/2020/the-social-consequences-of-non-consensual-pornography/> [https://perma.cc/N8JC-CUBR].

23 *Id.*

24 Senthil Amudhan et al., “Snapping, Sharing, and Receiving Blame”: A Systematic Review on Psychosocial Factors of Victim Blaming in Non-Consensual Pornography, Nt’l Inst. of Health (February 2024), <https://pmc.ncbi.nlm.nih.gov/articles/PMC11155645/> [https://perma.cc/9HMK-NLXA].

25 *Id.*

26 McKoy, *supra* note 22.

27 *Id.*

28 Murça et al., *supra* note 20.

29 Valerie A. Lapointe et al., *The Present and Future of Adult Entertainment: A Content Analysis of AI-Generated Pornography Websites*, Nt’l Inst. of Health (3 March 2025), <https://pubmed.ncbi.nlm.nih.gov/40032709/> [https://perma.cc/8BNW-YRR9].

30 Cassidy Gibson et al., *Analyzing the AI Nudification Application Ecosystem*, USENIX Sec. Symp., 2 (13 August 2025), <https://www.usenix.org/system/files/usenixsecurity25-gibson.pdf> [https://perma.cc/GM49-WCRZ].

the eyes and lips, haircut, age, and other physical attributes”.³¹ Many applications have an undressing tool, clothing changes, human-assisted AI undressing, face-swapping, image enhancers and more.³² Many of these applications do not require the user to sign in before prompting or generating content.³³

Nudification and face-swapping applications are new, and there are few studies regarding their impact and accessibility. Most applications/websites ask users if they are at least eighteen years old, some show nude content before requiring age confirmation and some sources do not verify the user’s age at all. In one study, only seven out of twenty analysed applications required that the image subject be over eighteen.³⁴ Half of the sources in this study state, before generation or in the terms and conditions, that the user *must* obtain consent from the image subject before nudification; the other half do not have any language requiring consent.³⁵

Nudification platforms attempted to advertise on Meta platforms, and Meta sued the firm behind one platform to force them to cease posting advertisements.³⁶ The Director of Global Safety Policy at Meta emphasized how the company aims to get ahead of “merely responding to harmful content by giving users more control over their online privacy”, like a service allowing users to report harmful content.³⁷ How this method differs from current social media reporting guidelines is not specified.³⁸ While social media platforms attempt to ban this content, AI platforms like ChatGPT are working to “treat adult users like adults” through erotic content that can be accessed after the user proves they are over eighteen years old.³⁹

4. International Approaches

The European Union’s (EU) framework demonstrates the importance of consistent definitions and advocates for “a consistent and high level of protection of public interests” and “common rules for high-risk AI systems”.⁴⁰ Europe has addressed child sexual exploitation in various ways, including Directive 2011/93/EU, “which

31 Thuy Thu Nguyen et al., *Impact of Perceived Benefits and Risks on Face Swap Applications Usage Intentions*, Sage Journals (29 August 2025), <https://journals.sagepub.com/doi/epub/10.1177/21582440251367590>.

32 Gibson et al., *supra* note 30, at 10.

33 *Id.*, at 7.

34 *Id.*, at 8.

35 *Id.*

36 Tom Gerken, *Meta Urged to Go Further in Crackdown on ‘Nudify’ Apps*, BBC (12 June 2025), <https://www.bbc.com/news/articles/cgr58dlne5o> [<https://perma.cc/X4N3-4S3W>].

37 Alina Ladyzhensky, *What Can Be Done to Prevent and Resist Image-based Abuse?*, Univ. of Pennsylvania: Annenberg Sch. for Commc’n (20 December 2021), <https://www.asc.upenn.edu/news-events/news/what-can-be-done-prevent-and-resist-image-based-abuse> [<https://perma.cc/YG2F-U75Q>].

38 *See id.*

39 Lily Jamali and Liv McMahon, *ChatGPT Will Soon Allow Erotica for Verified Adults, Says OpenAI Boss*, BBC (15 October 2025), <https://www.bbc.com/news/articles/cpd2qv58yl5o> [<https://perma.cc/5Y7M-3AQZ>].

40 *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonized Rules on Artificial Intelligence and Amending Regulations*, EUR-Lex (13 June 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> [<https://perma.cc/8CPZ-CVSE>].

mandates member states to adopt measures against the sexual abuse and exploitation of children and child pornography”.⁴¹ With the rise of deepfakes and other AI-generated pornography, the European Parliament published a statement, “Children and deepfakes”, discussing how the European Union (EU) can protect its children through legislation and education.⁴² One solution proposed by the European Parliament is for parents to “educate their children about the risks of deepfakes and ensure they implement strong privacy settings on their social media accounts”.⁴³ The statement discusses how OpenAI has launched an initiative “to detect deepfakes with a tool capable of distinguishing between AI-generated images and real ones”.⁴⁴ However, underreporting limits the data available to train detection tools, and the advancement of AI generators is much faster than the detection tools can learn.⁴⁵

Regulation 2024/1689 (the EU AI Act) is a single instrument that establishes consistent rules for AI systems across the European Union and imposes specific obligations on providers and deployers of certain categories of AI-generated content.⁴⁶ The EU AI Act states that “Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated”.⁴⁷ The EU AI Act “established transparency obligations to label such content (human-generated v. synthetic)” and “sets specific obligations for labelling deepfake content with the goal of ensuring transparency and preventing manipulation of the public”.⁴⁸

Article 50 of the EU AI Act – Transparency Obligations for Providers and Deployers of Certain AI Systems (Art. 50) – governs transparency obligations directly relevant to deepfakes.⁴⁹ Article 50 states that “deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated”.⁵⁰ The EU AI Act places the majority of compliance obligations on providers (those who bring AI systems to market) rather than on end-users.⁵¹ This

41 *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA*, EUR-Lex (13 December 2011), <https://eur-lex.europa.eu/eli/dir/2011/93/oj/eng> [<https://perma.cc/VSZ3-EE8P>].

42 *Children and Deepfakes*, European Parliament, 5 (July 2025), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf) [<https://perma.cc/7K55-C9CJ>].

43 *Id.*, at 4.

44 *Understanding the Source of What We See and Hear Online*, OpenAI (7 May 2024), <https://openai.com/index/understanding-the-source-of-what-we-see-and-hear-online/> [<https://perma.cc/TEP2-UGJW>].

45 *See Children and Deepfakes*, *supra* note 42, at 1.

46 *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonized Rules on Artificial Intelligence and Amending Regulations*, *supra* note 44.

47 *Id.*

48 *Id.*

49 *Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems*, EU Artificial Intelligence Act, <https://artificialintelligenceact.eu/article/50/> [<https://perma.cc/CVH4-MAP9>] (last accessed 3 June 2026).

50 *Id.*

51 *High-level Summary of the AI Act*, EU Artificial Intelligence Act (27 February 2024), <https://artificialintelligenceact.eu/high-level-summary/> [<https://perma.cc/U4RS-QFSQ>].

is a structural choice that mirrors the upstream-liability model this article advocates for in the United States.

Directive 2024/1385 (the “Violence Against Women Directive”) is the EU instrument most analogous to the U.S. criminal statutes on NDII.⁵² The Violence Against Women Directive specifies, for all Articles, that liability may attach “irrespective of whether the victim consented to the generation of the material or might have transmitted it to a particular person”.⁵³ This forecloses the defence that prior consent to create or share intimate material implies consent to public distribution. Article 5 of the Violence Against Women Directive discusses the criminalization of NDII/NCII.⁵⁴ Under Article 5, the following is punishable as a criminal offence: making NDII/NCII accessible to the public without the person’s consent, “where such conduct is likely to cause serious harm to that person”; “producing, manipulating, or altering, and subsequently making accessible to the public” NDII/NCII without the person’s consent, “where such conduct is likely to cause serious harm to that person”; and threatening to engage in the above conduct.⁵⁵

The European Parliament advocates for legislation to address the advancement of deepfakes.⁵⁶ The statement cites how China has “mandated that all AI-generated content be watermarked for the purpose of combating AI disinformation, but not for other purposes” and that the United Kingdom has “updated its Online Safety Bill to provide better protection for victims of deepfake abuse, making it illegal to create simulated child abuse, not just to share it”.⁵⁷ The European Parliament stresses the need for education in K-12 schools over legislation in this arena, because education leads to awareness and understanding of “the impacts of deepfakes” and can “contribute to making online users less prone to manipulation”.⁵⁸ As a result, “the European Commission and the Organisation for Economic Co-operation and Development (OECD) are working on an AI literacy framework, whose “final version will be released in 2026 to support educators in integrating AI literacy into their teaching practices”.⁵⁹

5. U.S. Federal Framework

(a) The Violence Against Women Act Reauthorization Act of 2022

The Violence Against Women Act (VAWA) was reauthorized in 2022 to include “provisions to address cybercrime and the nonconsensual dissemination of inti-

52 *Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence*, EUR-Lex (14 May 2024), <https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng> [https://perma.cc/3X4M-MXPE].

53 *Id.*

54 *Id.*

55 *Id.*

56 *Id.*

57 *Children and Deepfakes*, *supra* note 42, at 6.

58 *Id.*, at 7.

59 *New AI Literacy Framework to Equip Youth in an Age of AI*, OECD Education and Skills Today (29 April 2025), <https://oecdeditoday.com/new-ai-literacy-framework-to-equip-youth-in-an-age-of-ai/> [https://perma.cc/579K-G6ES].

mate pictures”.⁶⁰ The reauthorization created a right of action for “individuals who have an intimate image shared without their consent”, and the perpetrator knows or recklessly disregards that the individual has not consented to the publication of the image.⁶¹ This law allows the court to award damages and injunctive relief, while allowing the plaintiff to remain anonymous.⁶²

Title XIV of the VAWA 2022 Reauthorization Act created a grant programme to assist “state, tribal, and local law enforcement” in addressing cybercrimes against individuals and another grant to found the National Resource Center on Cybercrimes Against Individuals; however, Congress has not appropriated funds for these purposes.⁶³ Title XIV mandates that the Attorney General “develop a national strategy to address these types of crimes”.⁶⁴

(b) The TAKE IT DOWN ACT

The federal government has attempted to regulate authentic intimate visual depictions and digital forgeries through the TAKE IT DOWN Act, which became Public Law 119-12 on 19 May 2025.⁶⁵ The TAKE IT DOWN Act

prohibits the nonconsensual online publication of intimate visual depictions of individuals, both authentic and computer-generated, and requires certain online platforms to promptly remove such depictions upon receiving notice of their existence.⁶⁶

The TAKE IT DOWN Act applies to individuals and “covered platforms”.⁶⁷

There are four key provisions of the TAKE IT DOWN Act: (1) criminalization of NCII and threats to publish, (2) mandated swift removal from platforms, (3) protection of those acting in good faith and (4) preservation of free speech.⁶⁸ Covered platforms are websites, online services, online applications or mobile applications that serve the public and “primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files” or

for which it is in the regular course of trade or business of the website, online service, online application, or mobile application to publish, curate, host, or make available content of nonconsensual intimate visual depictions.⁶⁹

60 The 2022 Violence Against Women (VAWA) Reauthorization, Pub. L. No. 117-103, 136 Stat. 49 (2022).

61 *Id.*

62 *Id.*

63 *Id.*

64 *Id.*

65 TAKE IT DOWN Act, S. 146, 119th Congr. (2025).

66 *Id.*

67 *Id.*

68 TAKE IT DOWN Act, RAINN (28 August 2025), <https://rainn.org/federal-legislation/take-it-down-act/> [<https://perma.cc/H66Y-9P5G>].

69 TAKE IT DOWN Act, *supra* note 65.

The TAKE IT DOWN Act prohibits online publication of intimate visual depictions of adult subjects “where publication is intended to cause or does cause harm to the subject”, when publication is nonconsensual or “in the case of an authentic depiction, was created or obtained under circumstances where the adult had a reasonable expectation of privacy”.⁷⁰ The TAKE IT DOWN Act also prohibits online publication of intimate visual depictions of minor subjects “where publication is intended to abuse or harass the minor or to arouse or gratify the sexual desire of any person”.⁷¹ The TAKE IT DOWN Act also clarifies that consent to create or share an image or depiction with another individual does not mean consent to publish the image or depiction.⁷² The TAKE IT DOWN Act only targets the “knowing publication of NCII” and protects groups like “medical professionals, law enforcement, and others who disclose NCII responsibly and ethically” for investigative and other defined purposes.⁷³

Violators who commit an offence against an adult subject can be fined, imprisoned for up to two years or both; violators who commit an offence against a minor can be fined, imprisoned for up to three years or both.⁷⁴ The TAKE IT DOWN Act also criminalizes threats to commit an offence “for the purpose of intimidation, coercion, extortion, or to create mental distress”.⁷⁵ Violators of this section who commit an offence against an adult subject can be fined, imprisoned for up to eighteen months or both; violators who commit an offence against a minor can be fined, imprisoned for up to thirty months or both.⁷⁶

The TAKE IT DOWN Act outlines a “Notice and Removal of Nonconsensual Intimate Visual Depictions” that requires websites and online platforms to create a process for victims or an authorized person acting on their behalf can report these incidents within one year after the enactment of the TAKE IT DOWN Act.⁷⁷ Under this process, covered platforms must: (1) remove NCII within forty-eight hours of a victim’s verified request, (2) make reasonable efforts to remove any duplicates or reposts of the content and (3) provide a “clear and conspicuous notice” on the platform of the notice and removal process.⁷⁸

Under the TAKE IT DOWN ACT, platforms are not liable for any claims regarding the platform’s “good faith disabling of access to, or removal of, material”.⁷⁹ Essentially, platforms where these materials are posted cannot be held liable unless they do not take reasonable steps to dispose of or disable access to the NDII after a victim reports the images or depictions. The TAKE IT DOWN Act does not contain a pre-emption clause, allowing for state and federal law to work concurrently and

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.*

⁷³ TAKE IT DOWN Act, RAINN, *supra* note 68.

⁷⁴ TAKE IT DOWN Act, *supra* note 65.

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.*

provide more avenues for victims to seek protection.⁸⁰ The Federal Trade Commission (FTC) enforces the TAKE IT DOWN ACT, allowing the FTC to regulate how platforms handle AI.⁸¹

(c) The Disrupt Explicit Forged Images and Non-Consensual Edits Act

The federal government has also attempted “to improve rights to relief for individuals affected by non-consensual activities involving intimate digital forgeries, and for other purposes” through the Disrupt Explicit Forged Images and Non-Consensual Edits Act (DEFIANCE Act).⁸² The DEFIANCE Act would answer an important question regarding the TAKE IT DOWN Act – whether there is a right to federal action for digital forgeries.⁸³ The DEFIANCE Act amends Section 1309 of the Consolidated Appropriations Act to include “Nonconsensual Activity Involving Digital Forgeries” and defines digital forgery as

any intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.⁸⁴

The DEFIANCE Act entitles victims to the same relief regardless of whether the perpetrator used an authentic image or a digital forgery, thereby providing clarity and consistency.⁸⁵ The DEFIANCE Act has passed the Senate and was received by the House on 24 July 2024 but has not made any progress since then.⁸⁶

6. State Framework

(a) Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act

The National Conference of Commissioners on Uniform State Laws proposed the Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act (UCRUDIIA) to provide civil remedies for victims of NDII.⁸⁷ UCRUDIIA states that

80 David Leibert, *Congress's Attempt to Criminalize Nonconsensual Intimate Imagery: The Benefits and Potential Shortcomings of the TAKE IT DOWN Act*, Nt'l Ass'n of Att'ys Gen. (26 August 2025), <https://www.naag.org/attorney-general-journal/congresss-attempt-to-criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/> [https://perma.cc/B2LA-9E8T].

81 *Id.*

82 DEFIANCE Act, S. 3696, 118th Congr. (2024).

83 Leibert, *supra* note 80.

84 DEFIANCE Act, *supra* note 82.

85 *Id.*

86 *Id.*

87 Uniform Civil Remedies of Unauthorized Disclosure of Intimate Images Act, Nt'l Conf. of Comm'rs on Unif. State Laws (2019).

a depicted individual who is identifiable and who suffers harm from a person's intentional disclosure or threatened disclosure of an intimate image that was private without the depicted individual's consent has a cause of action against the person if the person knew [or acted with reckless disregard for whether]: (1) the depicted individual did not consent to the disclosure; (2) the intimate image was private; and (3) the depicted individual was identifiable.⁸⁸

UCRUDIIA protects reasonable expectations of privacy, those who consented to the creation of the image, those who previously consented to the image, and images created when an individual was in a public place.⁸⁹ Victims may recover (1) compensatory damages, economic and non-economic, including damages for emotional distress or statutory damages of up to \$10,000 against each defendant; (2) equal to any monetary gain made by the defendant for the NDII and punitive damages.⁹⁰ Victims may also be awarded attorney's fees and additional relief, including injunctive relief.⁹¹

UCRUDIIA is similar to the TAKE IT DOWN Act; however, UCRUDIIA does not explicitly discuss authentic images versus digital forgeries.⁹² Additionally, UCRUDIIA has a four-year statute of limitations and starts the timer for minors when they reach the age of majority; the TAKE IT DOWN Act does not specify a statute of limitations.⁹³ Numerous states have adopted the UCRUDIIA in its entirety since its proposal, including Washington, Colorado, Nebraska and South Dakota.⁹⁴

(b) Indiana Code § 35-45-4-8

The Indiana General Assembly passed House Bill 1047 – which provided protections for computer-generated intimate images of minors – as Public Law 79 (Indiana Code § 35-45-4-8) on 12 March 2024.⁹⁵ The legislature enacted Indiana Code § 35-45-4-8 under a declared emergency due to the rise in incidents of minors using AI to create NDII of other minors.⁹⁶ Indiana Code § 35-45-4-8 defined “computer generated image”, included computer-generated images under the pre-existing NDII law and expanded the law to include images that are “of a quality, characteristic, or condition such that it appears to depict the alleged victim”.⁹⁷ Indiana Code § 35-45-4-8 also expanded the law to include anyone “who knowingly or intentionally peeps in or into an area”, and they reasonably expect the victim to

88 *Id.*

89 *Id.*

90 *Id.*

91 *Id.*

92 See Uniform Civil Remedies of Unauthorized Disclosure of Intimate Images Act, *supra* note 87.

93 *Id.*

94 *Bill Analysis H.B. 1165*, Washington State House of Representatives Civil Rights and Judiciary Committee (18 January 2023), <https://lawfilesexternal.wa.gov/biennium/2023-24/Htm/Bill%20Reports/House/1165%20HBA%20CRJ%2023.htm#:~:text=The%20UCRUDIIA%20has%20been%20adopted,wrongful%20disclosure%20of%20intimate%20images> [https://perma.cc/VY7T-Z7X3].

95 H.B. 1047, 123rd Gen. Assemb., Reg. Sess. (Ind. 2024).

96 Mithani, *supra* note 4.

97 Ind. Code § 35-45-4-8 (2024).

“disrobe or is actually expected to disrobe” like restrooms.⁹⁸ Indiana Code § 35-45-4-8 explicitly exempts media, entertainment and internet platforms from liability when users create or publish NDII.⁹⁹ Under Indiana Code § 35-45-4-8, it is not necessary to prove the perpetrator actually sent the NDII.¹⁰⁰

State v. Katz was one of the first decisions that implemented Indiana Code § 35-45-4-8.¹⁰¹ In *Katz*, the defendant took a video of his girlfriend performing oral sex on him without her knowledge and sent the video to his ex-girlfriend.¹⁰² The defendant claimed Indiana Code § 35-45-4-8 was unconstitutional and violated the First Amendment of the U.S. Constitution.¹⁰³ The Indiana Supreme Court held that the defendant’s expressive act was an “abuse” of his rights under the First Amendment because it caused significant harm.¹⁰⁴ The Indiana Supreme Court stated that

the statute was a content-based restriction on speech but survived strict scrutiny due to the State’s compelling interest in preventing the serious harm caused by non-consensual dissemination of intimate images.¹⁰⁵

The court said, “nonconsensual pornography is a ‘unique crime fueled by technology’” because perpetrators can disseminate images with the click of a button, potentially providing identifying information, thereby amplifying views and the overall negative impact on victims.¹⁰⁶ While this case does not discuss a fact pattern with digital forgeries created with AI, it is essential to discuss because it provides a binding precedent of the law’s constitutionality and allows for future victims to obtain legal assistance.¹⁰⁷

B. Analysis/Arguments

I. Enforcement and Federal–State Interaction

Under Indiana Code § 35-41-1-1, a person may be convicted under Indiana law of an offence if they meet certain criteria; essentially, if the crime has a sufficient connection to Indiana, the person, then Indiana courts may try the individual.¹⁰⁸ A person who commits an offence under Indiana Code § 35-45-4-8 is subject to a Class A misdemeanour if they are a first-time offender; if the person has a prior

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ See *State v. Katz*, 179 N.E.3d 431 (2022).

¹⁰² *Id.*, at 439.

¹⁰³ *Id.*, at 440.

¹⁰⁴ *Id.*, at 456.

¹⁰⁵ *Indiana v. Katz*, Columbia Univ. Glob. Freedom of Expression, <https://globalfreedomofexpression.columbia.edu/cases/indiana-v-katz/> [https://perma.cc/6SXB-3UKM] (last accessed 30 October 2025).

¹⁰⁶ *State v. Katz*, *supra* note 101, at 449.

¹⁰⁷ *Indiana v. Katz*, *supra* note 105.

¹⁰⁸ Ind. Code § 35-41-1-1 (2024).

unrelated conviction, they are subject to a Level 6 felony.¹⁰⁹ Under Indiana Code § 35-50-3-2, “a person who commits a Class A misdemeanor shall be imprisoned for a fixed term of not more than one year” and may be fined up to \$5,000.¹¹⁰ If the person is subject to a Level 6 felony, they will be imprisoned between six months and three years and may be fined up to \$10,000.¹¹¹ In Indiana, courts do not typically sentence minors the same as adults, meaning that many minors may not receive jail time or penalties for their conduct.¹¹² Indiana Code § 35-33-10-3, known as the Uniform Criminal Extradition Act, essentially allows for people who live outside of Indiana to be held liable under Indiana law.¹¹³

The Cyber Civil Rights Initiative found that people who committed image-based sexual abuse reported that the threat of jail time was one of the strongest deterrents against committing the crime.¹¹⁴ Judges in juvenile court must weigh multiple factors, including “the severity of harm caused by deepfake abuse, the intent of the perpetrator, and adolescent psychology”.¹¹⁵

However, public policy is typically against minors being imprisoned or held to similar sentencing standards as adults.¹¹⁶ As such, policy solutions are essential to filling the gaps in education about the impact of NDII.¹¹⁷ Most minors may not know these images could have criminal consequences, so teaching students AI and digital literacy to demonstrate what “crosses the line into illegal behavior” can create conversations.¹¹⁸ Requiring courses on AI and digital literacy for minors that discuss the potential criminal liability for online conduct would allow schools and policymakers to focus on the core issues with NDII and other online behaviours: “consent, autonomy, agency, safety”.¹¹⁹ Additionally, providing resources for minors who have experienced NDII to report the offence is essential to keeping children safe and holding perpetrators accountable for their actions.¹²⁰

K-12 AI and digital literacy education can play a valuable supporting role in prevention efforts, but educational initiatives should complement, not replace, statutory and regulatory reform. Education alone will not quickly resolve or adequately address the structural problem created by commercially available nudification and face-swapping tools that enable abuse at scale. Effective reform

109 I.C. § 35-45-4-8 (2024).

110 Ind. Code § 35-50-3-2 (2024).

111 Ind. Code § 35-50-2-7 (2024).

112 *How Children Get to Juvenile Court*, Indiana Public Defender Council, <https://www.in.gov/ipdc/juvenile-justice/information-for-youth-and-parents/indiana-juvenile-justice-system/> [<https://perma.cc/LQT9-RXEZ>] (last accessed 30 October 2025).

113 Ind. Code § 35-33-10-3 (2024).

114 See Asia A. Eaton et al., 2017 *Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report*, Cyber Civil Rights Initiative (2017), <https://cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf> [<https://perma.cc/4D7V-MCNU>].

115 Mithani, *supra* note 4.

116 Richard Mendel, *Why Youth Incarceration Fails: An Updated Review of the Evidence*, The Sentencing Project (1 March 2023), <https://www.sentencingproject.org/reports/why-youth-incarceration-fails-an-updated-review-of-the-evidence/> [<https://perma.cc/6MR6-KY8Q>].

117 Mithani, *supra* note 4.

118 *Id.*

119 *Id.*

120 *Id.*

requires primary reliance on clear statutory definitions, platform accountability and upstream regulation of tool providers, with educational programming serving only as a secondary preventative measure that reinforces broader legal protections.

Indiana Code § 35-45-4-8 was written to go after “the person that’s actually creating this porn, not the medium that it actually gets placed on”, which means it does not account for platforms that allow users to generate NDII.¹²¹ Indiana’s omission of platform liability creates a critical enforcement gap that federal law only partially fills. The TAKE IT DOWN Act does not pre-empt state laws addressing NCII/NDII, which means victims have at least two avenues of protection.¹²² Under the TAKE IT DOWN Act, platforms are required to remove intimate visual depictions when the individual depicted requests and provide “clear and conspicuous notice” of its takedown procedure.¹²³ Because federal law requires platforms to remove intimate visual depictions, states will reap the benefits of this step towards accountability. States typically have a difficult time requiring platforms to create takedown procedures due to the First Amendment, and Congress has stepped in numerous times to assist with these difficulties.¹²⁴ Due to the TAKE IT DOWN Act, Indiana can hold platforms accountable when intimate visual depictions are not removed in a timely and reasonable manner.¹²⁵

The TAKE IT DOWN Act is geared towards platforms, yet it requires the victim to report the content before the platform is required to “take it down”. The TAKE IT DOWN Act fails to address a pressing issue: platforms legally provide nudification and face-swapping tools for consumers to use, typically for free and without an age restriction. Requiring platforms to remove content once it is reported is an ineffective solution because content can be generated faster than it can be removed through these processes. These tools have led to a surge in NDII in K-12 schools and beyond, and platforms should be held accountable across the country for the provision of tools that perpetuate sexual abuse.

II. *Expanding Liability to Platforms*

The central deficiency in Indiana law and the TAKE IT DOWN Act is a fundamental mismatch between where the harm originates and where the law intervenes. The current statutes operate downstream: punishing individual perpetrators after NDII has been created and distributed. The statutory requirements put the onus on the victim to report the NDII, and only once a report is made, is a platform required to remove the content. Neither statute touches the developers and operators of nudification and face-swap tools that make synthetic NDII generation possible. This gap reflects a deeply embedded assumption in U.S. technology law: that those

121 Brandon Smith, *Lawmakers Send Bill to Governor Criminalizing Computer-Generated Revenge Pornography*, IPB News (6 March 2024), <https://www.wfyi.org/news/articles/lawmakers-send-bill-to-governor-criminalizing-computer-generated-revenge-pornography> [https://perma.cc/J542-RLPE].

122 David Leibert, *supra* note 80.

123 TAKE IT DOWN Act, *supra* note 68.

124 Peter Benson et al., *Social Media: Regulatory, Legal, and Policy Considerations for the 199th Congress*, Congress (2025), <https://www.congress.gov/crs-product/IF12904> [https://perma.cc/3HQY-2ZQX].

125 David Leibert, *supra* note 80.

who provide tools bear no responsibility for the harms those tools enable. In an era where a perpetrator can search for an AI nudification tool and enter a prompt and generate NDII within minutes, that assumption can no longer be justified.

One key element of legislating this issue is distinguishing tool providers from covered platforms. The TAKE IT DOWN Act uses the term “covered platform” to describe websites and services that host user-generated content, such as social media platforms, where synthetic NDII circulates. Covered platforms are downstream of the harm, receiving and distributing content that has already been generated. Tool providers are entirely different actors: the developers and operators of nudification applications, face-swap services and so on. Tool providers create instruments of abuse and allow for synthetic NDII to be generated quickly and often at no cost to the perpetrator.

This distinction is essential. Current statutes in the United States dictate what covered platforms must do with NDII, but do not put duties on tool providers. Adopting legislation that prohibits nudification tools that lack age verification and consent verification would protect the rights of these tool providers, while protecting the safety and rights of victims. Additionally, Congress could require a watermark in every generated image so perpetrators can be identified more readily.

Congress could impose age verification requirements on tool providers as a condition of operating an image generation service. A systematic study of twenty nudification websites found that some sites allowed image generation without **any** confirmation that the user was eighteen or older.¹²⁶ In this study, only seven of the twenty examined sites required affirmation that the image subject was an adult immediately upon opening the website.¹²⁷ That failure is not a design oversight; it is a business choice that harms victims. A mandatory age verification addresses this harm and provides protection for minor victims.

Age verification alone is insufficient to resolve this for victims over eighteen years old. Congress could also require developers of nudification tools to add a consent verification mechanism. The same study of twenty nudification websites found that only half of the platforms examined included any language requiring users to obtain the image subject’s consent before generating content; these verifications were essentially unverifiable self-certifications.¹²⁸ A meaningful consent verification process would require tool providers to implement further protections, such as a manual review of all uploaded content or uploading an identification document.¹²⁹ These proposed requirements have inherent privacy trade-offs; however, if the user cannot provide this information, they likely do not have the consent of the person whose likeness they intend to use for content generation.¹³⁰ Lawful applications of nudification technology, including but not limited to consensual adult content creation, body visualization tools and medical imaging, would not be prohibited under the proposed regulations. A consenting

126 Cassidy Gibson et al., *supra* note 30, at 8.

127 *Id.*

128 *Id.*, at 3.

129 *Id.*, at 14.

130 *See id.*, at 8.

adult who wishes to use such a tool for legitimate purposes loses nothing from a consent verification requirement; only the nonconsensual use case is foreclosed.

Lastly, Congress would require an embedded watermark in each image generated by the tool providers' system, identifying which tool was used, a timestamp and a unique session identifier. In this circumstance, a watermark would provide a "recognisable and unique signal that serves to identify the content as AI-generated".¹³¹ This would provide victims with enhanced downstream protection through a traceable image generation process, allowing victims to obtain damages and press charges more accurately. The European Parliament has pointed to China's AI watermarking mandate as an example of how this could work long-term.¹³² Requiring watermarks on generated images provides victims and tool providers with the necessary information to pursue charges, damages and further protections.

Upstream obligations directed at tool providers do not prohibit speech; they impose design and verification requirements on a commercial service as a condition of operating. That is precisely the kind of conduct regulation that survives even heightened scrutiny, as courts have consistently recognized in contexts from commercial broadcasting to pharmaceutical advertising. Section 230 Immunity and Generative Artificial Intelligence (Section 230) protects providers of "interactive computer services" from liability for content created by third parties.¹³³ AI tools are "software applications that use artificial intelligence algorithms to perform tasks that typically require human intelligence, such as analyzing data, recognizing patterns, personalizing learning experiences, automating tasks, and making decisions".¹³⁴ AI tool providers are the organizations and entities that create and distribute these software applications.¹³⁵

AI tools perform tasks; they do not host third-party content. This means tool providers currently fall outside of Section 230, yet these providers are unregulated. Courts have consistently held that Section 230 does not immunize a platform for content it materially contributes to or helps create.¹³⁶ As such, a tool provider running an image through its nudification model is the creator of the resulting synthetic image, not a passive conduit.

These protections look at where the laws in the United States fail to protect victims. Currently, the TAKE IT DOWN Act requires the victim to discover that the NDII exists and then initiate a reporting process. Upstream obligations prevent

131 *Generative AI and Watermarking*, European Parliament, 2 (December 2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI\(2023\)757583_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf) [<https://perma.cc/AM5V-DR2S>].

132 *Id.*, at 1.

133 Section 230 Immunity and Generative Artificial Intelligence, S. 1993, 118th Congr. (2023).

134 *AI and Teaching and Learning: AI Tools and AI Technologies*, Univ. of Southern California (23 August 2025), <https://libguides.usc.edu/c.php?g=1457247&p=10880482> [<https://perma.cc/LDC9-X34N>].

135 *See EU Artificial Intelligence Act, Article 3: Definition*, Future of Life Institute (2 February 2025), <https://artificialintelligenceact.eu/article/3/> [<https://perma.cc/FJK2-527J>].

136 *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008); *Bouck v. Meta Platforms, Inc.*, No. 3:25-cv-05194, 2026 U.S. Dist. LEXIS 62626 (N.D. Cal. 24 March 2026).

some portion of that content from being generated and shift much of the burden to the tool providers rather than the victims.

Combining the current requirements for covered platforms with requirements for tool providers adds another layer of protection for victims and can slow the surge in technology-facilitated sexual abuse.

III. Expansion of Indiana Code § 35-45-4-8

The National Conference of Commissioners on Uniform State Laws proposed UCRUDIIA to provide civil remedies for victims of NDII.¹³⁷ When comparing UCRUDIIA to Indiana Code § 35-45-4-8, noticeable gaps appear in Indiana's current protections for victims. Under UCRUDIIA, multiple terms are explicitly defined: consent, depicted individual, identifiable, identifying characteristic, individual, intimate image and more.¹³⁸ UCRUDIIA defines "depicted individual" as "an individual whose body is shown in whole or in part in an intimate image".¹³⁹ I.C. § 35-45-4-8 does not define this term; nor does it use this term; rather, I.C. § 35-45-4-8 uses multiple phrases to describe a "depicted individual": individual, person and alleged victim.¹⁴⁰ They also use "person" to describe an alleged perpetrator, decreasing clarity for a reader, as none of these terms are defined or differentiated.¹⁴¹

Additionally, Indiana Code § 35 does not define consent in any section, despite defining numerous terms in "Chapter 2. Definitions" and throughout Indiana Code § 35.¹⁴² Indiana should adopt UCRUDIIA's consistent language and adopt "depicted individual" as a term used throughout the statute to reference the individual harmed (or allegedly harmed) and should move its consent definition to the "Chapter 2. Definitions" section of the Indiana Code to ensure it is easily defined and understood in Indiana Code § 35-45-4-8.

UCRUDIIA defines "identifiable" as

recognizable by a person other than the depicted individual: (A) from an intimate image itself; or (B) from an intimate image and identifying characteristic displayed in connection with the intimate image.¹⁴³

Indiana Code § 35-45-4-8 does not define "identifiable"; nor does it use "identifiable" at any point in the statute.¹⁴⁴ Nor does Indiana Code § 35-45-4-8 define "identifying characteristic"; instead, it discusses conduct "that is of a quality, characteristic, or condition such that it appears to depict the alleged victim".¹⁴⁵ UCRUDIIA defines "identifying characteristic" as "information that may be used to

137 Uniform Civil Remedies of Unauthorized Disclosure of Intimate Images Act, *supra* note 87.

138 *Id.*

139 *Id.*

140 Ind. Code § 35-45-4-8 (2024).

141 *See id.*

142 Ind. Code § 35 (2024).

143 Uniform Civil Remedies of Unauthorized Disclosure of Intimate Images Act, *supra* note 87.

144 Ind. Code § 35-45-4-8 (2024).

145 *Id.*

identify a depicted individual”.¹⁴⁶ Again, the absence of these important definitions in Indiana Code § 35-45-4-8 can lead to confusion for victims and offer perpetrators broader protection because the language in I.C. 35-45-4-8 puts qualifiers on identifiable information like “quality, characteristic, or condition”.¹⁴⁷

Crimes like NDII are incredibly sensitive, and consistent, clear language is essential for victims to feel secure in knowing they have protections under the law; when laws for rape were unclear, many types of serious sex crimes were not embodied in statutes, and victims suffered as a result.¹⁴⁸ Adopting language from UCRUDIIA will prevent statutory ambiguity because terms will be defined and consistently used throughout the legislation.

IV. Recommendations for Legislators

Indiana’s statute closely follows the American tradition of regulating individual actors rather than the technological infrastructure that facilitates their misconduct. I.C. § 35-45-4-8 imposes criminal penalties on those who create or distribute intimate images without consent, including synthetic images, but explicitly exempts online platforms from liability.¹⁴⁹ The TAKE IT DOWN Act similarly imposes obligations only after an image has been disseminated, requiring platforms to remove reported content within forty-eight hours.¹⁵⁰ Neither statute restricts access to nudification tools, deepfake applications or other generative AI systems capable of producing synthetic NDII.¹⁵¹ These frameworks share a foundational weakness: reliance on victim reporting and post-incident remedies rather than prevention. While civil and criminal penalties may deter some adult offenders, they do not meaningfully constrain the technical environment in which synthetic NDII is produced.

By contrast, European regulatory initiatives embrace intervention at the platform level. The EU AI Act requires GAI distributions to include technical markers signalling AI origin and compels platforms to implement systems for detecting and mitigating sexually exploitative deepfakes.¹⁵² Violence Against Women Directive criminalizes the nonconsensual sharing of intimate images, including deepfakes, and expressly covers “images, photographs, and videos”, “sexualised images”, “audio clips” and “video clips”.¹⁵³ Together, these measures

146 Uniform Civil Remedies of Unauthorized Disclosure of Intimate Images Act, *supra* note 87.

147 See Ind. Code § 35-45-4-8 (2024).

148 Cynthia L. Cooper, *Words Matter: How Language Reflects Our Response to Sexual Violence*, A.B.A. (12 February 2025), https://www.americanbar.org/groups/diversity/women/publications/perspectives/2015/winter/how_language_reflects_our_response_sexual_violence/ [https://perma.cc/88BS-ZXLS].

149 See I.C. § 35-45-4-8.

150 TAKE IT DOWN Act, *supra* note 68.

151 See I.C. § 35-45-4-8; TAKE IT DOWN Act, *supra* note 68.

152 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, *supra* note 52.

153 *Id.*

recognize that synthetic NDII is not solely user misconduct but a foreseeable consequence of readily available AI tools capable of generating exploitative content.

The EU framework's treatment of consent further strengthens victim protections in ways the U.S. law does not. Violence Against Women Directive specifies that liability may attach "irrespective of whether the victim consented to the generation of the material or might have transmitted it to a particular person".¹⁵⁴ This clarification eliminates a common defence argument that prior consent to create or share intimate material implies consent to public dissemination. Indiana Code § 35-45-4-8 does not provide the same degree of explicit clarification, which may disadvantage victims who had consented to the generation but not the distribution of intimate content.¹⁵⁵

Definitional inconsistency compounds these structural problems. Ambiguity throughout legislative efforts introduces interpretive uncertainty and creates opportunities for inconsistent enforcement. UCRUDIIA represents a promising domestic model for definitional clarity and has been adopted in several states. The EU AI Act and European Parliament similarly employ standardized definitions, providing consistent expectations for providers, platforms and regulators. Taken together, UCRUDIIA and the EU's definitional structures demonstrate how a federal definitional framework in the United States would enhance interstate enforcement, facilitate cooperation with platforms and improve the clarity and accessibility of legal protections for victims.

A regulatory model that incorporates platform liability and technical safeguards, such as watermarks and consent verification, could substantially reduce harm. Congress could adopt such measures by requiring nudification, face-swap and other similar tool platforms to implement age verification systems, meaningful consent verification procedures and embedded watermarking requirements for generated content. This upstream model would translate effectively into U.S. law because it does not prohibit lawful expression outright; rather, it regulates the commercial design and deployment of technologies that foreseeably facilitate exploitation.

As a secondary complement to these legal reforms, prevention may also extend into educational settings. The EU Parliament's discussion of NDII and AI-generated content focuses deeply on educating K-12 students and advocates for structured education on digital consent, privacy and the consequences of AI-generated content. Such educational components could reduce the prevalence of peer-to-peer NDII more effectively than criminal penalties alone and would likely teach students how to report NDII, increasing reporting rates and data around NDII.

What does not translate directly is the EU's member-state implementation structure, which has no federal analogue; in the United States, the appropriate vehicle is a federal statute that pre-empts inconsistent state definitions while preserving state criminal jurisdiction, mirroring the TAKE IT DOWN Act's existing non-pre-emption structure. The EU model thus offers the United States a proof of

¹⁵⁴ *Id.*

¹⁵⁵ See I.C. § 35-45-4-8.

concept: upstream design obligations and downstream criminal liability are not in tension, and a jurisdiction can implement both within a coherent legal framework.

Indiana's statutes illustrate the limits of state-level action in a domain defined by global platforms, cross-border distribution and commercially available AI tools that no state can effectively regulate on its own. The EU's combined regulatory framework acts as a demonstrative template for coherent legal architecture in this ever-evolving field of law. A federal statute that pairs clear, uniform definitional standards with upstream obligations on tool providers would replicate that structure and provide relief to victims. The EU framework shows that these reforms are not only possible, but compatible.

C. Conclusion

This article has argued for two reforms: (1) clear, uniform statutory definitions and (2) upstream regulation of tool providers. Comparative approaches from the EU AI Act and Directive 2024/1385 illustrate how transparency obligations, platform-level safeguards and upstream design requirements can prevent harm before it occurs. K-12 digital literacy education, while valuable, should serve as a secondary complement to these structural reforms rather than a primary solution. Together, these frameworks suggest that effective NDII prevention in the United States requires a coordinated strategy that combines state innovation with federal uniformity, platform accountability and education.

Indiana Code § 35-45-4-8 represents an important step towards addressing the rise of AI-generated intimate imagery, yet the statute's inconsistent terminology, lack of clear definitions, and exemption of platforms limit its effectiveness in a digital environment where nudification and deepfake tools remain widely accessible. Models such as UCRUDIIA demonstrate the value of definitional precision, while federal initiatives like the TAKE IT DOWN Act offer improved takedown mechanisms, but only after victims report the harm. As a result, current U.S. law places the burden on victims without imposing meaningful obligations on the technological infrastructure that enables synthetic NDII. The EU framework's comparative advantage lies precisely in its uniformity and consistency: the AI Act establishes a single definitional and compliance baseline that applies identically across all twenty-seven member states, eliminating the interpretive fragmentation that undermines enforcement when perpetrators and platforms operate across jurisdictions.

A federal approach in the United States modelled on the EU's definitional and structural coherence would close the enforcement gaps that jurisdictional inconsistency currently creates and provide victims with protections that do not depend on where they happen to live. Consistency and clarity are essential when discussing AI and technological advances because the landscape is always evolving. Without laws that cover a broad range of harmful conduct in the NDII space and beyond, victims can struggle to bring perpetrators to justice. Legislators have a responsibility to address ongoing concerns of NDII in K-12 schools and beyond with compassion, consistency and clarity.