



Volume 53

Issue II: Spring 2026

**Better Than Revenge: A Comparative Analysis of New York and New Jersey’s
Legal Remedies for Revenge Porn and AI-Generated Explicit Content**

Courtney L. Stonefelt*

Table of Contents

I. INTRODUCTION 241

**II. THE TAYLOR SWIFT INCIDENT: A CASE STUDY IN AI-GENERATED
REPUTATIONAL HARM..... 245**

**III. HISTORICAL DEVELOPMENT OF PRIVACY RIGHTS IN IMAGE-BASED
SEXUAL ABUSE..... 247**

**IV. ANALYSIS OF CURRENT REVENGE PORN STATUTES IN NEW JERSEY AND
NEW YORK..... 251**

V. ANALYSIS OF DEFAMATION LAW IN NEW JERSEY AND NEW YORK 257

VI. THE FEDERAL TAKE IT DOWN ACT 262

VII. CONCLUSION 266

I. INTRODUCTION

On March 15, 2022, the mother of an anonymous woman was contacted through social media private message.¹ When opening the message, the mother was confronted with an image of her naked daughter, “breasts and genitals in full view.”² The images were sent from the anonymous woman’s (the plaintiff) ex-lover.³ The messages included “outside links containing additional images and videos of [the] plaintiff” which were sent to both the “plaintiff’s mother [and] business associates” of the woman.⁴ This anonymous woman’s story represents one instance of an increasingly prevalent form of sexual abuse that has devastated countless lives across the United States. Recent statistics from the Cyber Civil Rights Initiative reveal that one in twelve adult Americans have been victims of nonconsensual distribution of intimate images and that one in eight adult social media users have been targets of nonconsensual distribution of intimate images, or nonconsensual pornography.⁵

Nonconsensual pornography is “defined as the distribution of sexually graphic images of individuals without their consent (also known as “revenge porn,” “cyber rape,” and [“image-based sexual abuse”]).”⁶ Nonconsensual pornography includes “images originally obtained without consent (e.g., hidden recordings or recordings of sexual assault) as well as images originally obtained with consent.”⁷ Revenge porn is a type of nonconsensual pornography.⁸ Revenge porn typically consists of consensual images or videos “given to an intimate partner who later distributes

* J.D. Candidate, Rutgers Law School, 2026.

¹ P.F. v Brown, 2024 NY Slip Op 51356 (U), *1–2 (N.Y. Sup. Ct., Queens County 2025).

² *Id.*

³ *Id.*

⁴ *Id.* (internal quotations omitted).

⁵ See generally CYBER CIV. RTS. INITIATIVE, <https://cybercivilrights.org/> (last visited Mar. 17, 2025).

⁶ Asia A. Eaton, et al., *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report*, CYBER CIV. RTS. INITIATIVE, 3 (June 2017), <https://cybercivilrights.org/wp-content/uploads/2017/06/CCRI-20>.

⁷ Danielle K. Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014).

⁸ *Id.*

them without consent.”⁹ “Revenge porn presents serious consequences for its victims. It disproportionately affects women and girls compared to boys and men, and female revenge pornography victims frequently endure many of the same negative mental health consequences as rape survivors.”¹⁰

The negative mental health consequences of revenge porn extend far beyond momentary embarrassment, and often result in severe and lasting trauma. Research from the Cyber Civil Rights Initiative indicates that victims frequently experience “worse mental health outcomes and higher levels of physiological programs than non-victims.”¹¹ Victims experience “mental health effects such as depression and anxiety, job loss or problems securing new employment, and offline harassment and stalking.”¹² A study in 2017 “supports the idea that nonconsensual pornography has many of the same health consequences for victims as in-person sexual assault.”¹³ In looking at 18 revenge porn survivors, the participants “reported posttraumatic stress disorder, anxiety, depression, suicidal thoughts, [and] other negative mental health outcomes as a result of their victimization.”¹⁴ Many “are dismissed from their current employment and/or struggle to find work. . . they leave jobs, change schools, retreat from public discourse . . . all of which can lead to further serious adverse consequences for their family, social, [and] professional [] lives.”¹⁵ This psychological devastation is worsened by the persistent nature of digital content, where victims may face continuous re-traumatization as images resurface or remain accessible online.

⁹ *Id.*

¹⁰ Zachary Starks-Taylor & Jamie Miller, *Politicians Live on Camera: Revenge Porn, Elections, and the First Amendment*, 99 N.Y.U. L. REV. 158, 160 (2024).

¹¹ Eaton, et al., *supra* note 6, at 23.

¹² Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, 12 FEMINIST CRIMINOLOGY 22, 23 (2017).

¹³ Yanet Ruvalcaba and Asia A. Eaton, *Nonconsensual Pornography Among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men*, AMERICAN PSYCH. ASS’N, 3 (Dec. 14, 2018).

¹⁴ *Id.*

¹⁵ Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 2017 OXFORD J. OF LEGAL STUD., 12 (Jan. 31, 2017).

In 2015, major steps were taken to combat the dissemination of revenge porn by removing “many of the primary websites hosting nonconsensual porn, like IsAnyoneUp or U Got Posted,” and major companies like Facebook and Google “incorporate[ing] ways for victims to have nonconsensual porn removed from their platforms.”¹⁶ Additionally, substantial legal changes occurred as almost every state enacted some sort of statutory recourse, except for Massachusetts and South Carolina.¹⁷ The nation’s first revenge porn statute was enacted in New Jersey in 2004 through N.J.S.A. 2C:14-9.¹⁸ Over a decade later, New York followed suit and implemented similar protections in 2019 through NY Penal Law §245.15.¹⁹ However, despite these significant steps, the problem has only increased. “In 2016, 10 million people, or 2% of Americans, had reported being victims of nonconsensual porn.”²⁰ In 2019, there was a 400% increase from the number of victims in 2016 (50 million people).²¹

Despite the already existing challenges of combating revenge porn, it has only become exponentially more complex with the emergence of artificial intelligence. New AI technologies are capable of generating hyper-realistic explicit images, known as “deepfakes,” completely from scratch. “A deepfake is an artificial image or video (a series of images) generated by a special kind of *machine learning* called “deep” learning,” also known as artificial intelligence.²² “Deep learning is similar to any kind of machine learning, where an algorithm is fed examples and learns to produce output that resembles the examples it learned from.”²³ This algorithm can produce

¹⁶ *An Update on the Legal Landscape of Revenge Porn*, NAT'L ASS'N OF ATTY'S GEN. (Nov. 16, 2021), <https://www.naag.org/attorney-general-journal/an-update-on-the-legal-landscape-of-revenge-porn/>.

¹⁷ *Nonconsensual pornography (revenge porn) laws in the United States*, BALLOTPEDIA (Mar. 18, 2025, 12:00AM), [https://ballotpedia.org/Nonconsensual_pornography_\(revenge_porn\)_laws_in_the_United_States](https://ballotpedia.org/Nonconsensual_pornography_(revenge_porn)_laws_in_the_United_States).

¹⁸ *Id.*

¹⁹ N.Y. Penal Law §245.15.

²⁰ NAT'L ASS'N OF ATTY'S GEN., *supra* note 16.

²¹ *Id.*

²² *What the heck is a deepfake?*, UNIV. OF VA INFO. SEC. (Mar. 18, 2025, 12:03AM), <https://security.virginia.edu/deepfakes>.

²³ *Id.*

manipulated video, image, or audio that appears convincingly realistic. This deep learning can make someone appear to say or do something they never actually said or did. With this evolution of technology, an innocent image taken from Instagram can be manipulated to produce a realistic, explicit pornographic image, with “some remov[ing] a person’s clothes or superimpose[ing] a person’s face over another’s to depict them saying something they did not [], and some are entirely generated by AI.”²⁴ These creations pose significant risk to personal privacy and reputation, as well as challenge existing legal frameworks designed to protect individuals from non-consensual intimate image sharing. Nothing underscores more the potential for AI’s harm and the depth of image circulation on social media and the Internet than the recent incident of AI-generated explicit content targeted at Taylor Swift.²⁵

This article will examine the legal and procedural frameworks of revenge porn statutes and defamation laws in New York and New Jersey. This article will discuss how these statutes apply to traditional revenge porn but will primarily focus on their applicability to AI-generated explicit content and deepfakes. In examining these legal frameworks, the article will identify critical gaps in legal protection against deepfakes. Despite the progressive nature of enacting specific statutes to target revenge pornography, the New York and New Jersey laws provide inadequate protection against the emerging threat of AI-generated explicit content. This analysis proceeds in several parts. First, we will look at the Taylor Swift incident in depth, using it as a marker of the capabilities of artificial intelligence technology. Then we will trace the historical legal development of privacy rights, beginning with Warren and Brandeis’s conceptualization of the

²⁴ Blake Montgomery, *Taylor Swift AI images prompt US bill to tackle nonconsensual, sexual deepfakes*, THE GUARDIAN, (Jan. 30, 2024) <https://www.theguardian.com/technology/2024/jan/30/taylor-swift-ai-deepfake-nonconsensual-sexual-images-bill>.

²⁵ “Sexualized, exaggerated images of Swift at football games went viral over the weekend on X, racking tens of millions of views, according to Twitter’s metrics.” *Id.*

right to privacy. Part IV examines the effectiveness of revenge pornography statutes in New York and New Jersey and the current legislative approaches in New Jersey and New York, while Part V does the same for defamation law. Our analysis will conclude with an examination of a newly introduced federal revenge pornography bill, the “Tools to Address known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act” (TAKE IT DOWN Act, S. 4569).”

As technology continues to evolve, the law must adapt to provide protection against emerging forms of image-based abuse. The harm these victims experience, like that of the anonymous plaintiff above, extends beyond temporary emotional distress, oftentimes resulting in long-term professional, personal, and psychological injury.²⁶

II. THE TAYLOR SWIFT INCIDENT: A CASE STUDY IN AI-GENERATED REPUTATIONAL HARM

In January 2024, social media users were inundated by the widespread circulation of “fake, sexually explicit images” purporting to be of mega superstar Taylor Swift and the Kansas City Chiefs NFL team.²⁷ The images, created using AI technology, “spread rapidly across social media platforms,” particularly X (formerly Twitter).²⁸ Within hours, the AI-generated explicit content had been viewed millions of times, with “one image shared by a user on X viewed 47 million times before the account was suspended.”²⁹ The fast dissemination of these images sparked a firestorm of demands to address this awful situation.³⁰

²⁶ See generally Bates, *supra* note 12, at 23.

²⁷ Kate Conger & John Yoon, *Explicit Deepfake Images of Taylor Swift Elude Safeguards and Swamp Social Media*, N.Y. TIMES (Jan. 26, 2024), <https://www.nytimes.com/2024/01/26/arts/music/taylor-swift-ai-fake-images.html>.

²⁸ *Id.*

²⁹ *Id.*

³⁰ See Montgomery, *supra* note 24; see also Conger & Yoon, *supra* note 27.

The images of Swift first appeared on the online messaging board, 4chan, and were also disseminated through the instant message platform, Telegram.³¹ From these platforms they very quickly spread to mainstream social media platforms, amassing “tens of millions of views.”³² In an effort to stop the rapid dissemination, “Swifties³³ began flooding X with tweets of the phrase “Taylor Swift AI” accompanied by clips of her performing to stymie searches for the images.”³⁴ Despite the Swifties efforts, nothing could stop the shares, comments, and likes on the posts. The engagement with the posts only pushed them further into the algorithm, causing them to show up on more individual feeds. As the images were fairly realistic, the incident sparked a lot of discussion about the advancing artificial intelligence technology and the looming dangers of AI-generated content.³⁵ As more news came out hour by hour about this massive distribution of AI-generated explicit images, “Elon Musk’s X took the drastic step of prohibiting all searches for Swift to contain the spread of the images.”³⁶ It’s no surprise that Musk’s action was largely due to the high-profile victim and the national media attention.³⁷ But even so, the damage was already done as the images had been seen by millions and likely downloaded by hundreds. The continued existence of digital content on the Internet was no match for even someone like Taylor Swift.³⁸

This incident raises grave concerns about how ordinary individuals might fare in similar situations. In fact, “4chan users who created the images of Swift did so as part of a “game” of sorts to see if they could craft lewd and sometimes violent visuals of famous women, from singers to

³¹ Emanuel Maiberg, *Microsoft Closes Loophole That Created AI Porn of Taylor Swift*, 404 MEDIA (Jan. 29, 2024), <https://www.404media.co/microsoft-closes-loophole-that-created-ai-porn-of-taylor-swift/>.

³² See Montgomery, *supra* note 24.

³³ Taylor Swift’s fanbase has come to be known as “Swifties.”

³⁴ Conger & Yoon, *supra* note 27.

³⁵ See Montgomery, *supra* note 24; see also Conger & Yoon, *supra* note 27.

³⁶ See Montgomery, *supra* note 24.

³⁷ *Deepfake explicit images of Taylor Swift spread on social media. Her fans are fighting back*, ASSOCIATED PRESS (Jan. 26, 2024), <https://apnews.com/article/taylor-swift-ai-images-protecttaylorswift-nonconsensual-d5eb3f98084bcbb670a185f7aeec78b1>.

³⁸ See Montgomery, *supra* note 24; Conger & Yoon, *supra* note 27.

politicians.”³⁹ While these viral pornographic images of Taylor Swift have garnered massive mainstream attention to AI-generated explicit content, “she is far from the only victim . . . In the 4chan community where these images originated, she isn’t even the most targeted public figure. This shows that anyone can be targeted in any way, from global celebrities to school children.”⁴⁰ This case study illustrates how rapidly and uncontrollably AI-generated content can spread throughout social media. These deepfake images can cause severe reputational harm and should serve as a reminder to urgently respond with effective legal remedies. “Although the imagery may be fake, the harm to the victims from the distribution of sexually explicit ‘deepfakes’ is very real.”⁴¹

III. HISTORICAL DEVELOPMENT OF PRIVACY RIGHTS IN IMAGE-BASED SEXUAL ABUSE

Our modern legal framework which protects individuals from image-based sexual abuse finds its theoretical foundations in Warren and Brandeis’s 1890 article, “The Right to Privacy.”⁴² Written in response to emerging “instantaneous photographs and newspaper enterprise[s] . . . invading the sacred precincts of private and domestic life . . .”, the article presented a distinct “right to be let alone.”⁴³ The focus of “The Right to Privacy” article is on existing property law as an inadequate protection for emotional and reputational harm caused by unwanted publicity.⁴⁴ The analysis presented by Warren and Brandies laid the foundation for understanding privacy as a fundamental right, which the Supreme Court later incorporated in its interpretation of the Substantive Due Process Clause.

³⁹ Kate Gibson, *Fake and graphic images of Taylor Swift started with AI challenge*, CBS NEWS (Feb. 5, 2024), <https://www.cbsnews.com/news/taylor-swift-artificial-intelligence-ai-4chan/>.

⁴⁰ *Id.*

⁴¹ Montgomery, *supra* note 24.

⁴² Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HAR. L. REV. 193 (1890).

⁴³ *Id.* at 195.

⁴⁴ *See generally id.*

In “The Right to Privacy,” Warren and Brandeis were concerned about photography’s potential for intrusion on privacy, which stemmed directly from unknown harms from technological developments of their era.⁴⁵ As they observed, “numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops.”⁴⁶ Their concerns about emerging technology potentially invading privacy still remains relevant today as we navigate the emergence of artificial intelligence and its ability to create intimate images without actual physical intrusion. The “Right to Privacy” article is significant because it acknowledges that privacy goes beyond physical property rights of common law and encompasses psychological and personal interests as well. Warren and Brandeis emphasize that “the principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy,” and goes on to argue that this principle should be extended “to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.”⁴⁷ As technology advances, “solitude and privacy have become more essential to the individual.”⁴⁸

The developing right to privacy gained significant momentum in the mid-twentieth century with a few groundbreaking Supreme Court decisions. First, in *Griswold v. Connecticut*, the Court recognized a fundamental right to privacy within “penumbras” and “emanations” of various constitutional protections, namely the First, Third, Fourth, and Ninth Amendments, creating a “zone of privacy.”⁴⁹ While *Griswold*’s holding specifically addressed the right to contraception, the opinion stands for a broader proposition recognizing the individual right to privacy in intimate,

⁴⁵ *Id.*

⁴⁶ *Id.* at 195 (internal quotations omitted).

⁴⁷ *Id.* at 213.

⁴⁸ Warren & Brandeis, *supra* note 42, at 213..

⁴⁹ *Griswold v. Connecticut*, 381 U.S. 479, 484-85 (1965).

sex-related matters.⁵⁰ *Griswold* laid the foundation for later cases to build upon these principals of personal autonomy and intimate relationships. The Court further developed this principle in *Stanley v. Georgia*, in holding that the First and Fourteenth Amendments prohibit making the “mere possession of printed or filmed [obscene material] in the privacy of a person’s own home” a crime.⁵¹ The Court in *Stanley* further stated that “if the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.”⁵² This holding established important precedent for modern privacy rights in the digital sphere. Taken together, these cases protect sexual autonomy and provide support for legal protection to combat revenge porn, which fundamentally violates these privacy interests.

Looking more closely at the relationship between technology and privacy, the digital revolution fundamentally transformed the nature of privacy violations. In *Carpenter v. United States*, while addressing the key issue of a Fourth Amendment search to access cell phone records, Chief Justice Roberts opines how “expectations of privacy form around new technology often will be difficult to determine during periods of rapid technological change.”⁵³ This point by the Chief Justice essentially states that technology has created privacy concerns that the drafters of the Fourth Amendment could never have anticipated.⁵⁴ Although the issue of revenge porn does not particularly pertain to the Fourth Amendment’s search and seizure protections, the underlying issue of privacy and emerging technology discussed in the opinion could be applicable to revenge porn and AI-generated explicit content. The ability to instantly distribute and permanently preserve

⁵⁰ *Id.* at 479.

⁵¹ *Stanley v. Georgia*, 394 U.S. 557, 564 (1969).

⁵² *Id.* at 565.

⁵³ *Carpenter v. United States*, 585 U.S. 296, 338 (2018).

⁵⁴ *Id.*

intimate images creates what many have termed “digital permanence,” which is a state where privacy violations potentially exist in perpetuity. The Court in *Riley v. California* further emphasizes this point of digital privacy in its holding that the government may not conduct a warrantless search of a cell phone upon arrest.⁵⁵ The Court notes here that “modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.”⁵⁶ The Court held that allowing police to search cell phone “records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.”⁵⁷ The Court’s articulation of privacy protections in Fourth Amendment searches provides further support for enhanced legal frameworks in addressing digital privacy violations of AI-generated explicit content.

The Court further shaped the development of privacy rights by upholding privacy of intimate moments and personal autonomy. As articulated in *Lawrence v. Texas*, the Constitution protects “the most private human conduct, sexual behavior, and in the most private of places, the home.”⁵⁸ Nevertheless, the current privacy frameworks remain inadequate to address the unique harms of digital sexual privacy violations, as argued by legal scholar Danielle Keats Citron in “Sexual Privacy.”⁵⁹ For Citron, “sexual privacy sits at the apex of privacy values because of its

⁵⁵ *Riley v. California*, 573 U.S. 373 (2014).

⁵⁶ *Id.* at 393.

⁵⁷ Further stating that “the storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.” *Id.* at 395.

⁵⁸ *Lawrence v. Texas*, 539 U.S. 558, 567 (2003).

⁵⁹ “Despite sexual privacy’s importance, reforms have proceeded slowly. This is partly because we lack a clear conception of what sexual privacy is and the harms wrought by its invasion. Policy makers and companies have addressed particular abuses only in isolation. One day, the discussion centers on nonconsensual pornography; the next,

importance to sexual agency, intimacy, and equality. . . [w]e are free only insofar as we can manage the boundaries around our bodies and intimate activities.”⁶⁰

The latest challenge to privacy is the emergence of artificial intelligence capable of generating realistic explicit images. This technological development echos Warren and Brandeis’s concerns about technological advancements outpacing legal protections.⁶¹ More specifically, AI-generated content raises novel questions regarding privacy when no *actual* intimate image exists but is rather completely fabricated. This challenges current conceptions of privacy rights, as the substantive due process right to privacy presumes actual private moments, images, or situations, not something completely fabricated.

As the capability for technology to invade privacy has expanded, the law’s ability to provide adequate protection has lagged. By understanding the history of the right to privacy and how that has expanded to current statutes, we can begin to develop further a more effective response to revenge porn, and more specifically to AI-generated explicit content.

IV. ANALYSIS OF CURRENT REVENGE PORN STATUTES IN NEW JERSEY AND NEW YORK

In 2004, New Jersey became the first state to combat non-consensual pornography by enacting N.J.S.A. 2C:14-9.⁶² New Jersey was a pioneer in criminalizing revenge pornography, and that statute’s early adoption reflects New Jersey’s recognition of the psychological harm from sexual exploitation.⁶³ A few years after the enactment of the statute, this potential harm became extremely relevant when Tyler Clementi, a first-year student at Rutgers University, ended his own

it centers on sextortion; and so on. Because the full breadth of the harm is not in view, policy makers fail to realize the costs of those violations.” Danielle Keats Citron, *Sexual Privacy*, 128 YALE L. J. 1870, 1875 (2019).

⁶⁰ *Id.* at 1874.

⁶¹ See generally Warren & Brandeis, *supra* note 42, at 213.

⁶² N.J.S.A. §. 2C:14-9.

⁶³ Tal Kopan, *States criminalize ‘revenge porn,’ POLITICO* (Oct. 30, 2013), <https://www.politico.com/story/2013/10/states-criminalize-revenge-porn-099082>.

life due to online sexual exploitation.⁶⁴ Clementi hosted a date in his dorm room and, without Clementi's consent, his roommate livestreamed his date.⁶⁵ "The roommate, and those who watched online, mocked, ridiculed, and harassed [Clementi] online and via social media because of his sexuality."⁶⁶ Tyler later learned of the livestream through social media and tragically ended his own life by suicide.⁶⁷ After years of lobbying and advocacy from victims' rights organizations and newspapers sharing stories similar to Clementi's, New York enacted its revenge porn statute, NY Penal Law §245.15⁶⁸, in 2019.⁶⁹

New Jersey's statute takes a broad approach to criminalizing non-consensual pornography. N.J.S.A. 2C:14-9(c) provides that:

an actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he discloses any photograph, film, videotape, recording or any other reproduction of the image taken in violation of subsection b. of this section of: (1) another person who is engaged in an act of sexual penetration or sexual contact; (2) another person whose intimate parts are exposed; or (3) another person's undergarment-clad intimate parts, unless that person has consented to such disclosure.⁷⁰

⁶⁴ *Tyler Clementi Ctr.*, RUTGERS DIV. OF ACCESS AND CMTY. ENGAGEMENT, <https://nbaccess.rutgers.edu/learn-grow/clementi-center/tylers-story>.

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ N.Y. Penal Law § 245.15.

⁶⁹ Gabrielle Fonrouge & Bernadette Hogan, *Cuomo signs historic bill outlawing revenge porn in New York*, NEW YORK POST (Jul. 23, 2019), <https://nypost.com/2019/07/23/new-york-state-enacts-historic-bill-to-crack-down-on-revenge-porn/>.

⁷⁰ N.J.S.A. § 2C:14-9(c)(1). For purposes of subsection (c), "disclose means sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, disseminate, present, exhibit, advertise, offer, share, or make available via the Internet or by any other means, whether for pecuniary gain or not."

Subsection (b) of the statute builds on the concept of reasonable expectation of privacy. The New Jersey Supreme Court expands on this in *Friedman v. Martinez* by stating, “imagine a secret camera in a bedroom used by a married couple. Someone who hides a recording device there intrudes on and disrupts their privacy, even if the couple cannot locate any video evidence. The harm occurs when the electronic invasion of privacy takes place, so long as the intrusion would be highly offensive to a reasonable person.”⁷¹ This “reasonable expectation of privacy” extends to intimate images shared within the context of a romantic relationships, even if initially shared consensually.

New York’s more recent statute, while building on lessons learned from earlier legislation like New Jersey’s, takes a somewhat different approach. Under NY Penal Law §245.15, “a person is guilty of unlawful dissemination or publication of an intimate image [revenge porn] when”⁷²:

(a) with intent to cause harm to the emotional, financial or physical welfare of another person, they intentionally disseminate or public a still or video image depicting such other person with one or more intimate parts exposed or engaging in sexual conduct with another person, including an image created or altered by digitization, where such person may reasonably be identified from the still or video image itself or from information displayed in connection with the still or video image; and (b) the actor knew or reasonably should have known that the person depicted did not consent to such dissemination or publication, including the dissemination or publication of an image taken with the consent of the person depicted when such person had a reasonable expectation that the image would

⁷¹ *Friedman v. Martinez*, 242 N.J. 449, 470 (2020).

⁷² N.Y. Penal Law § 245.15.

remain private, regardless of whether the actor was present when such image was taken.⁷³

“Penal Law § 250.40 defines disseminate as "to give, provide, lend, deliver, mail, send, forward, transfer or transmit, electronically or otherwise to another person.”⁷⁴ The same statute defines “publish” as an action:

(a) to disseminate [as previously defined] with the intent that such image or images be disseminated to ten or more persons; or (b) disseminate with the intent that such images be sold by another person; or (c) post, present, display, exhibit, circulate, advertise or allows access, electronically or otherwise, so as to make an image or images available to the public; or (d) disseminate with the intent that an image or images be posted, presented, displayed, exhibited, circulated, advertised or made accessible, electronically or otherwise and to make such image or images available to the public.⁷⁵

The New York statute notably includes specific intent requirements which are absent from New Jersey’s law. The element of intent requires that prosecutors prove the defendant intended to cause harm, that is, that the defendant had the appropriate mens rea or mental state. The Criminal Court held in *People v. Marvel B.* that “merely disseminating an image is insufficient to sustain the charge . . . the dissemination must also be unlawful.”⁷⁶ The Criminal Court relies on the legislative history of the statute to further explain:

⁷³ *Id.*

⁷⁴ *People v. Marvel B.*, 84 Misc. 3d 430, 433 (2024) (*citing* N.Y. Penal Law §250.40(5)).

⁷⁵ *Id.* (*citing* N.Y. Penal Law §250.40(6)).

⁷⁶ “To establish this, the People are required to set forth facts which substantiate the element that the defendant's dissemination was done with the intent to cause the complaining witness harm to her emotional, financial or physical welfare. Factual allegations that allege that the defendant sent the complainant intimate images of herself are insufficient alone to sustain the element of an intent to cause harm.” *Marvel B.*, 84 Misc. 3d at 434.

The Legislature, in enacting Penal Law § 245.15, never intended to criminalize the dissemination of intimate images among parties in a relationship. Rather, the purpose of the statute was to criminalize the conduct of a party who chose to share these intimate images outside the relationship. This conduct "also known as 'revenge porn' is often provided to Internet websites, and features photos sometimes accompanied by disparaging descriptions and identifying details . . . Posting these photographs online is damaging to the reputations of the victims." (Assembly Mem in Support, Bill Jacket, L 2019, ch 109 at 6.) The conduct becomes illegal when disseminating the intimate images to the public, friends or family to embarrass, hurt, harm or damage the complaining witness's reputation. The Legislature's commentary makes clear that dissemination of the intimate images to the public with the intent to harm the complaining witness is what is criminal, not sending the images, taken with the complainant's consent, to the complainant.⁷⁷

The two states differ significantly in their approaches to penalties. New Jersey classifies violation of their revenge pornography statutes as a third-degree crime, punishable by three to five years in prison and fines up to \$15,000.⁷⁸ New York's statute classifies violations as class A misdemeanors, which carry potential sentences of up to one year in jail.⁷⁹ Amendments to the New York statute have enhanced penalties for repeat offenders and cases involving minors.⁸⁰

The New York and New Jersey statutes were both drafted before the AI-technological boom, and therefore, without artificial intelligence in mind, resulting in significant challenges

⁷⁷ *Id.* at 434-35.

⁷⁸ *Revenge Porn Crimes and Penalties NJ 2C:14-9*, THE TORMEY LAW FIRM, LLC (Mar. 18, 2025, 12:45 a.m.), <https://criminallawyerinnj.com/revenge-porn-crimes-and-penalties-nj-2c14-9/#:~:text=Civil%20Ramifications,their%20income%20and%20financial%20worth.>

⁷⁹ N.Y. Penal Law § 245.15.

⁸⁰ *Id.*

when applied to AI-generated explicit content. It is clear from their language that the statutes were drafted with traditional photography and videography in mind, as well as partner-related intimate image sharing.⁸¹ It is significant, however, to note that New York Penal Law §245.15 does include the language “created or altered by digitization.”⁸² This language inclusion appears to allude to technological changes in the future and is notably absent from New Jersey’s statute.⁸³ This might potentially provide a stronger foundation for cases involving AI-generated explicit content, but nevertheless, there has yet to be a case in New York that specifically addresses the issue of AI-generated explicit content. So, how the New York courts will interpret “created or altered by digitization” in consideration of artificial intelligence technology is a question that remains open.

However, even with New York’s progressive thinking and broad statutory language, there appears to still be some legal challenges in applying the revenge porn statute to AI-generated explicit content. For example, NY Penal Law §245.15 requires that the dissemination be completed “with intent to cause harm to the emotional, financial or physical welfare of another person.”⁸⁴ This intent requirement presumes a partner relationship. By placing the harm in the dissemination of the image and not the creation of the image, the emphasis is on the reasonable expectation that the image should remain private, not that the image should not have been created in the first place. This language operates on the “scorned partner” premise alone, where the ex-lover feels such deep resentment over the relationship that he releases his ex’s nudes to friends or online. In this scenario, there is a clear chain of custody of the image from its creation to its dissemination. In AI-generated explicit content, that chain of custody does not exist as there is no image ever “taken” in the

⁸¹ N.J.S.A. § 2C:14-9; N.Y. Penal Law § 245.15.

⁸² N.Y. Penal Law § 245.15.

⁸³ N.J.S.A. § 2C:14-9.

⁸⁴ *Id.*

traditional sense. Even if investigators can track down the creator on a 4chan messaging board, can they prove an intent to harm?

In further analyzing the statutory language, both N.J.S.A. 2C:14-9 and NY Penal Law §245.15 require “reproduction” of an image to prove dissemination.⁸⁵ N.J.S.A. 2C:14-9 specifically refers to “photograph, film, videotape, recording, or other *reproduction* of the image of another.” Similarly, NY Penal Law §245.15 defines an “intimate image” as “a photograph, film, videotape, recording or any other *reproduction* of an image of a depicted individual.”⁸⁶ This language suggests the need for the capture of an *original* intimate moment to later be reproduced and disseminated. But AI-generated images are their own creations. There is no original moment or image that is copied. AI technology has the ability to completely fabricate a private moment, creating an entirely fake image. If AI technology lacks a reproduction element, it may place AI content outside the scope of revenge porn statutory protection.

V. ANALYSIS OF DEFAMATION LAW IN NEW JERSEY AND NEW YORK

An individual’s reputation within their community is paramount to living a happy and successful life. In the event of another making false statements to diminish a plaintiff’s standing within that community, defamation claims are the key protection. In fact, the defamation laws in New York and New Jersey may offer an alternative remedy to victims of AI-generated explicit content. The Restatement (Second) of Torts defines a defamatory communication as one that “tends to damage another’s reputation to the extent of lowering their regard in the community or

⁸⁵ *Id.*; N.Y. Penal Law §245.15.

⁸⁶ *People v. Mowring*, 2019 NY Slip Op 29209, 906 (N.Y. Crim. Ct. 2019).

detering others from associating with them.”⁸⁷ Both New York and New Jersey have adopted this definition.⁸⁸

At first, it seems that applying defamation law to revenge porn may seem conceptually problematic because defamation traditionally requires falsity and revenge porn typically involves authentic images of intimate moments. However, for traditional revenge porn involving authentic images, defamation claims can rely on the theory that nonconsensual dissemination of images creates false implications about the victim.⁸⁹ As articulated in *Milkovich v. Lorain Journal Co.*, even literally true statements can be defamatory when they imply false assertions of fact.⁹⁰ In the traditional revenge porn context, this means that perhaps the unauthorized distribution of the intimate image may falsely imply the victim consented to public distribution. Alternatively, defamation claims may be a more straightforward remedy for AI-generated explicit content, since the AI-generated images are fabricated and false images.⁹¹

Under New York law, defamation arises from a false statement which exposes the victim “to public contempt, ridicule, aversion or disgrace, or induce[s] an evil opinion of him in the minds of right-thinking persons, and to deprive him of their friendly intercourse in society.”⁹² To establish a claim for defamation in New York, the plaintiff must prove the following elements: “(1) a false statement about the complainant, (2) published to a third party without authorization or privilege, (3) through fault amounting to at least negligence on the part of the publisher⁹³, and (4) that neither

⁸⁷ RESTATEMENT (SECOND) OF TORTS § 559 (AM. LAW INST. 1977).

⁸⁸ *Hyman v. Rosenbaum Yeshiva of North Jersey*, 258 N.J. 208 (2024); *Zuckerbrot v. Lande*, 75 Misc 3d 269 (Sup. Ct., NY County 2022).

⁸⁹ *Milkovich v. Lorain J. Co.*, 497 U.S. 1 (1990).

⁹⁰ *Id.*

⁹¹ *See supra* Introduction (describing deepfakes).

⁹² *Sydney v. MacFadden Newspaper Pub. Corp.*, 242 N.Y. 208, 211-12 (1926).

⁹³ In cases involving public figures, such as the incident with Taylor Swift, the law requires an additional element of “actual malice.” *LaNasa v. Stiene*, No. 22-cv-5686, 2024 U.S. Dist. LEXIS 70340, at*20 (E.D.N.Y. Apr. 17, 2024). This standard requires the plaintiff to “allege sufficient facts to support a reasonable inference that the defendant made the statement with reckless disregard for the truth.” *Id.* Because this article is focusing more on the average person

constitutes defamation per se or caused ‘special damages.’”⁹⁴ Defamation can be in the form of words, pictures, or drawings.⁹⁵ The New York Supreme Court held in *Metzger v. Dell Pub. Co.* that a complaint alleging unauthorized use of plaintiffs’ photograph, which held them up to public ridicule, disgrace, and humiliation, stated a cause of action for libel.⁹⁶

New York courts have recognized that false portrayals of a person in sexually compromising situations can constitute defamation per se.⁹⁷ In *Nolan v. State*, a photograph model brought an action against the State for defamation, defamation per se, and violation of statutory right of privacy after the State used her photograph in an HIV education campaign. The court held that statements imputing HIV to a person are defamatory per se, recognizing that such statements can expose a person to public contempt, hatred, ridicule, aversion, or disgrace.⁹⁸ The court held that “a defamation plaintiff must plead special damages unless the defamation falls into any one of four per se categories: “(1) statements charging the plaintiff with a serious crime; (2) statements that tend to injure the plaintiff in her trade, business or profession; (3) statements that impute to the plaintiff a “loathsome disease”; and (4) statements that impute unchastity to a woman.”⁹⁹ AI-generated explicit images may constitute as defamation per se under at least one of these four categories, potentially relieving victims from the burden of proving special damages.

and not public figures, we will not be analyzing the malice element, as “a private figure need only allege that the defendant acted with negligence.” *Id.*

⁹⁴ *Jacob v. Lorenz*, 626 F. Supp. 3d 672, 686 (S.D.N.Y. 2022).

⁹⁵ *See generally* *Myers v. Afro-Am. Publ’g. Co.*, 5 N.Y.S.2d 223, 223 (N.Y. Sup. Ct. 1938), *aff’d*, 255 A.D. 838, 7 N.Y.S.2d 662 (App. Div. 1938); *see also* *Quezada v. Daily News*, 125 Misc. 2d 302 (N.Y. App. Term 1984) (holding that libel need not be in words but may take the form of a picture or drawing).

⁹⁶ *See generally* *Metzger v. Dell Publ’g. Co.*, 207 Misc. 182 (Sup. Ct., N.Y. County 1955); *see also* *Quezada*, 125 Misc.2d 302 (N.Y. App. Term 1984) (finding that if the picture brings a person into hatred, contempt, or ridicule, the publication of the picture will be actionable for libel); *see also* *Myers*, 168 Misc. 429 (N.Y. Sup. Ct. 1938) (holding that a photograph or pictorial representation which tends to expose the subject to public ridicule or contempt is just as effective a libel as the most studied form of words).

⁹⁷ *Nolan v. State*, 158 A.D.3d 186 (2018); *see also* *Laguerre v. Maurice*, 192 A.D.3d 44 (2020) (acknowledging that the false imputation of homosexuality could be considered defamation per se).

⁹⁸ *Nolan*, 158 A.D.3d at 186.

⁹⁹ *Id.* at 195; *see also* *Lieberman v. Gelstein*, 80 N.Y.2d 429, 435 (N.Y. 1992); *Harris v. Hirsh*, 228 A.D.2d 206, 208 (N.Y. App. Div. 1996).

In proving fault, New York courts set a high bar for public figures, holding that plaintiffs must prove “actual malice.”¹⁰⁰ Yet most of the 500 million Americans affected by image-based sexual abuse are not required to meet that standard, but rather must meet the standard of negligence.¹⁰¹ Despite the lower standard, proving negligence in the creation and distribution of AI-generated content presents unique challenges.¹⁰² The standard for negligence is “whether the defendant[] failed to exercise ordinary care in publishing false statements which defamed plaintiff, considering the foreseeable danger of injury from the publication and the reasonableness of defendants’ conduct in proportion to that danger.”¹⁰³ However, even under the standard of negligence, the plaintiff must have enough evidence and facts to properly show failure of ordinary care.¹⁰⁴ In an anonymous digital age, this is challenging, and likely impossible.

However, New York’s procedural rules create significant challenges. The one-year statute of limitations for defamation claims “runs from the date of the initial publication of the defamatory writing, and not from the date of the publication’s distribution,” or discovery of the publication.¹⁰⁵ This short timeframe may cause difficulty for victims who do not immediately discover the distribution of AI-generated images impersonating them. However, New York has adopted the single publication rule, which “reduces the possibility of hardship to plaintiffs by allowing the collection of all damages in one case commenced in a single jurisdiction.”¹⁰⁶ By contrast, a

¹⁰⁰ The plaintiff must prove “that the statement was made with ‘actual malice’ – that is, with knowledge that it was false or with reckless disregard of whether it was false or not.” *New York Times Co. v. Sullivan*, 376 U.S. 254, 280 (1964).

¹⁰¹ *Gottwald v. Sebert*, 40 N.Y.3d 240 (N.Y. 2023) (holding that the acceptable standard of liability for defamation involving private figures is negligence); *see also* *Ortiz v. Valdescastilla*, 102 A.D.2d 513 (N.Y. App. Div. 1984); *Krauss v. Globe Intern, Inc.*, 251 A.D.2d 191 (N.Y. App. Div. 1998).

¹⁰² *Gottwald*, 40 N.Y.3d 240 (N.Y. 2023).

¹⁰³ *Lee v. City of Rochester*, 663 N.Y.S.2d 738, 754 (N.Y. Sup. Ct., Monroe Cty. 1997); *see also* *Danielenko v. Kinney Rent A Car, Inc.*, 57 N.Y.2d 198, 204, (N.Y. App. Div. 1982) (“If the defendant could not reasonably foresee any injury as the result of his act, or if his conduct was reasonable in the light of what he could anticipate, there is no negligence, and no liability.”) (quoting *W. Prosser, The Law of Torts*, § 43, at 250 (4th ed. 1971)).

¹⁰⁴ *Lee*, 663 N.Y.S.2d at 754.

¹⁰⁵ *Rare 1 Corp. v. Moshe Zwiebel Diamond Corp.*, 822 N.Y.S.2d 375, 377 (N.Y. Sup. Ct., N.Y. County 2006).

¹⁰⁶ *Firth v. State*, 98 N.Y.2d 365, 370 (N.Y. 2002).

multiple publication rule “would implicate an even greater potential for endless retriggering of the statute of limitations, multiplicity of suits and harassment of defendants.”¹⁰⁷

In New Jersey, a defamation claim includes three elements: “(1) the assertion of a false and defamatory statement concerning another; (2) the unprivileged publication of that statement to a third party; and (3) fault amounting at least to negligence by the publisher.”¹⁰⁸ The court in *Govito v. West Jersey Health System, Inc.*, states that “a defamatory statement is one that is false and 1) injures another person’s reputation; or 2) subjects the person to hatred, contempt or ridicule; or 3) causes others to lose good will or confidence in that person.”¹⁰⁹

The negligence element in defamation cases requires that the defendant acted negligently in failing to ascertain the truth or falsity of the statement before communicating it.¹¹⁰ Negligence, in *Hyman v. Rosenbaum Yeshiva of North Jersey*, “is defined as conduct that creates an unreasonable risk of harm.”¹¹¹

Similar to New York, New Jersey’s statute of limitations for defamation is one year from the date of publication of the alleged defamatory statement.¹¹² Codified in N.J.S.A. 2A:14-3, “every action at law for libel or slander shall be commenced within 1 year net after the publication of the alleged libel or slander.”¹¹³ Also, in parallel with its “sister state” New York, New Jersey has adopted the single publication rule, which could be particularly beneficial in cases where false images have been shared multiple times across various platforms.¹¹⁴ This rule allows for the consolidation of claims as a “plaintiff alleging defamation has a single cause of action, which arises

¹⁰⁷ *Id.*

¹⁰⁸ *Hyman*, 258 N.J. at 236 (Patterson, J., concurring) (internal quotations omitted).

¹⁰⁹ *Govito v. W. Jersey Health Sys., Inc.*, 332 N.J. Super. 293, 305 (App. Div. 2000).

¹¹⁰ *NuWave Inv. Corp. v. Hyman Beck & Co., Inc.*, 432 N.J. Super. 539 (App. Div. 2013).

¹¹¹ *Hyman*, 258 N.J. at 238 (Patterson, J., concurring) (internal quotations omitted).

¹¹² *Smith v. Datla*, 451 N.J. Super. 82 (App. Div. 2017); *Beljakovic v. Longin*, No. A-5330-09 (App. Div. July 28, 2011).

¹¹³ N.J.S.A. § 2A:14-3 (2025).

¹¹⁴ See RESTATEMENT (SECOND) OF TORTS § 577A (AM. LAW. INST. 1977).

at the first publication of an alleged libel, regardless of the number of copies of the publication distributed or sold.”¹¹⁵ The court went even further in *Churchill* to “apply the single publication rule to Internet publications,” following the precedent of many other jurisdictions.¹¹⁶ This rule has the potentiality of simplifying the legal process for victims.

VI. THE FEDERAL TAKE IT DOWN ACT

In December 2024, Senate Bill 4569 passed the US Senate.¹¹⁷ The “Tools to Address known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act” (TAKE IT DOWN Act, S. 4569) represents a significant development in the legal landscape addressing revenge pornography and AI-generated explicit content.¹¹⁸ On May 19, 2025, President Trump signed into law the TAKE IT DOWN Act, marking “a landmark step in the fight to protect victims of digital exploitation.”¹¹⁹ The TAKE IT DOWN Act “is a bi-partisan bill that aims to protect victims of non-consensual intimate imagery [] which includes deepfakes, revenge porn, and other harmful attacks.”¹²⁰ As outlined above, both N.J.S.A. 2C:14-9 and New York’s Penal Law §245.15 contain limitations when applied to AI-generated explicit content.¹²¹ The TAKE IT DOWN Act directly confronts these state statute limitations by establishing definitions and mechanisms specifically targeting “digital forgeries” created through artificial intelligence.

¹¹⁵ *Churchill v. State*, 378 N.J. Super. 471 (App. Div. 2005).

¹¹⁶ Other courts have also applied the single publication rule to Internet publications. *See, e.g.*, *Van Buskirk v. N.Y. Times Co.*, 325 F.3d 87, 89–90 (2d Cir. 2003); *Lane v. Strang Communications Co.*, 297 F. Supp. 2d 897, 899–900 (N.D. Miss. 2003); *Mitan v. Davis*, 243 F. Supp. 2d 719, 721–24 (W.D. Ky. 2003); *Simon v. Ariz. Bd. Of Regents*, 28 Media Law Reports 1240, 1245–1246 (Ariz. Sup. Ct. 1999); *Traditional Cat Ass'n, Inc. v. Gilbreath*, 118 Cal. App. 4th 392, 394–405 (2004); *McCandliss v. Cox Enter., Inc.*, 593 S.E.2d 856, 858 (Ga. App. 2004), *reconsid. denied* (Feb. 2, 2004), *cert. denied* (May 24, 2004); *Abate v. Me. Antique Digest*, 2004 WL 293903, *1–2 (Mass. Sup. Ct. Jan. 26, 2004); *E.B. v. Liberation Publ'ns, Inc.*, 777 N.Y.S.2d 133, 134 (2004). *Cf.*, *Oja v. Fink*, 2003 WL 23996035, *4–5 (D. Or. Feb. 26, 2003); *Churchill v. State*, 378 N.J. Super. 471, 481 (App. Div. 2005).

¹¹⁷ S. 4569, 118th Cong. (2024).

¹¹⁸ *Id.*

¹¹⁹ *ICYMI: President Trump Signs TAKE IT DOWN Act into Law*, THE WHITE HOUSE (May 19, 2025) <https://www.whitehouse.gov/articles/2025/05/icymi-president-trump-signs-take-it-down-act-into-law/>.

¹²⁰ Priya Elangovan, *What to Know about the Take It Down Act*, ALL IN TOGETHER, (Mar. 7, 2025) <https://aitogether.org/what-to-know-about-the-take-it-down-act/>.

¹²¹ *See id.*; *supra* Part IV: Analysis of Current Revenge Porn Legislation in New Jersey and New York.

Both the New Jersey and New York statutes contain potential interpretive gaps when applied to AI-generated content. New Jersey’s N.J.S.A. 2C:14-9 refers narrowly to “photograph, film, videotape, recording, or other reproduction of the image of another,” while New York’s Penal Law §245.15 includes “an image created or altered by digitization.”¹²² Both statutes contain language suggesting the need for an “original” intimate moment that was captured, potentially excluding synthetic content that does not “reproduce” an actual image.¹²³ The TAKE IT DOWN Act directly addresses this limitation through its comprehensive definition of “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.”¹²⁴ This definition seemingly closes a significant gap in the state statutes aforementioned, as it explicitly encompasses content created through artificial intelligence, and does not require any reproduction of an original image. The Act further strengthens its definition by establishing a “reasonable person” standard. The Act covers any depiction that “when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.”¹²⁵ This reasonable person standard meaningfully captures AI-generated harm because it seems to focus on the *perceived* authenticity of the depiction rather than the *actual* authenticity, which traditional revenge porn statutes fail to do.¹²⁶

The analysis of New York’s revenge porn statute highlighted its specific intent requirement as potentially problematic for AI-generated content cases.¹²⁷ Under a specific intent requirement,

¹²² N.J.S.A. § 2C:14-9; N.Y. Penal Law § 245.15.

¹²³ See *supra* Part IV (discussing statutory construction limitations).

¹²⁴ S. 4569, 118th Cong. § 2(h)(1)(B).

¹²⁵ *Id.*

¹²⁶ See *supra* Part IV (discussing how the NY and NJ revenge porn statutes focus on the production and dissemination of real photographs and depictions).

¹²⁷ See *supra* Part IV.

prosecutors must prove that the defendant acted “with intent to cause harm to the emotional, financial or physical welfare of another person.”¹²⁸ As noted, this requirement might create evidentiary challenges in cases involving AI-generated images that lack the traditional “scorned partner” dynamic contemplated by the legislature.¹²⁹ The TAKE IT DOWN Act adopts a more flexible approach. For adult victims¹³⁰, Section 2(h)(3)(A)(iv) requires that the publication of a digital forgery either “is intended to cause harm *or* causes harm, including psychological, financial, or reputational harm, to the identifiable individual.”¹³¹

As previously discussed, there are difficulties in applying the “reasonable expectation of privacy” standard to AI-generated content since these types of images are not “captured” in the traditional sense and lack a clear chain of custody from creation to dissemination contemplated by the statutes.¹³² In focusing more specifically on the consent to publish issue rather than an expectation of privacy in the creation of the image, the TAKE IT DOWN Act avoids this problem. Section 2(h)(5) explicitly states that “the fact that the identifiable individual provided consent for the creation of the intimate visual depiction shall not establish that the individual provided consent for the publication of the intimate visual depiction.”¹³³ Section 2(h)(5) highlights the important distinction in AI-generated content that consent for creation of the image must be separated from consent for the publication and dissemination of the image. The Act creates a clear standard that is more applicable to deepfakes rather than traditional revenge porn.

¹²⁸ N.Y. Penal Law § 245.15(1)(a).

¹²⁹ See *supra* Part IV (discussing New York’s legislative history emphasizing the harm in the dissemination of an image that was taken with a reasonable expectation that the image would remain private).

¹³⁰ For minors, which this article does not discuss, the Act removes the harm requirement entirely, prohibiting publication of digital forgeries with intent to “abuse, humiliate, harass, or degrade the minor” or to “arouse or gratify the sexual desire of any person.” This approach recognizes the inherently harmful nature of such content involving minors, addressing a vulnerability in state statutes. S. 4569, 118th Cong. § 2(h)(3)(B).

¹³¹ S. 4569, 118th Cong. § 2(h)(3)(A)(iv).

¹³² See *supra* Part IV (discussing chain of custody challenges with AI-generated images).

¹³³ S. 4569, 118th Cong. § 2(h)(5).

In addition, the TAKE IT DOWN Act addresses quite specifically one of the core elements of defamation law; the need to prove reputational harm.¹³⁴ Section 2(h)(3)(A)(iv) of the Act creates a broader range of harms, including “psychological, financial, *or* reputational harm,” which better reflects the impact experienced by victims of AI-generated explicit content.¹³⁵ This aligns with the court’s reasoning in *Nolan v. State*, holding that fabricated portrayals of a sexual nature of an individual can satisfy defamation per se because of the image’s potential to expose the victim to “public contempt, hatred, ridicule, aversion, or disgrace.”¹³⁶

As examined earlier, there are significant procedural challenges with defamation claims, particularly regarding statutes of limitations periods. Both New York and New Jersey impose one-year limitation periods for defamation claims running from the date of publication rather than discovery, and both states have adopted the single publication rule for online content.¹³⁷ These short timeframes may be insufficient for victims of AI-generated content who may not immediately discover its distribution. The TAKE IT DOWN Act provides two significant improvements. First, as a federal criminal statute, it would presumably be subject to the general five-year statute of limitations applicable to non-capital federal offenses under 18 U.S.C. §3282.¹³⁸ The longer limitations period would allow victims substantially more time to discover and report violations. Second, and of particular importance to our discussion, the Act contains social media and website platform removal requirements that would create an immediate remedy for the victim, independent of any criminal prosecution.¹³⁹ That is, Section 3(a)(3) requires covered platforms to

¹³⁴ S. 4569, 118th Cong. § 2(h)(3)(A)(iv).

¹³⁵ *Id.*; *see supra* Introduction.

¹³⁶ *Nolan*, 158 A.D.3d at 195.

¹³⁷ *See supra* Part V: Defamation Law (discussing statutes of limitations and the single publication rule).

¹³⁸ 18 U.S.C. § 3282 (establishing five-year statute of limitations for non-capital federal offenses).

¹³⁹ *Id.*

remove flagged content within 48 hours of receiving a valid removal request and to make reasonable efforts to identify and remove known identical copies.¹⁴⁰

Despite the adoption of state statutes which were a significant development in protection against revenge porn, there are still many limitations regarding AI-generated explicit content. As seen above, the TAKE IT DOWN ACT attempts to address those limitations. Victims of AI-generated explicit content can pursue the state law claims where appropriate, while the government can pursue the criminal complaint addressing interstate distribution of deepfakes and removal requests. Although the TAKE IT DOWN Act does not solve all the problems facing victims of AI-generated explicit content, it does provide crucial new tools to address the current limitations in existing state remedies.

VII. CONCLUSION

Unfortunately, image-based sexual abuse will only continue to adapt and evolve with each new technological advance, constantly challenging existing legal standards and frameworks. Although the New York and New Jersey revenge porn statutes have made significant steps toward addressing this abuse, as outlined above, these statutes encounter severe limitations when confronted with AI-generated explicit content.¹⁴¹ Similarly, while defamation law shows a lot of promise in providing remedies for victims of deepfake content, most notably in the requirement to prove a *false* statement, defamation law does ultimately present procedural hurdles which might create substantial barriers in seeking relief.¹⁴² Just as Warren and Brandeis recognized in 1890 that “instantaneous photographs” necessitated new legal protections for privacy, today’s AI

¹⁴⁰ S. 4569, 118th Cong. § 3(a)(3).

¹⁴¹ See *supra* Part IV (analyzing the limitations of N.J.S.A. 2C:14-9 and NY Penal Law § 245.15 when applied to AI-generated content).

¹⁴² See *supra* Part V (discussing procedural challenges with defamation claims, particularly regarding statutes of limitations).

capabilities demand adaptive legal responses as well.¹⁴³ The Supreme Court’s progression from *Griswold*’s recognition of privacy in the right to contraception within the “penumbras” of The Constitution to *Carpenter*’s acknowledgment that “expectations of privacy form around new technology” directly illustrates how legal protections regarding privacy *will* attempt to evolve alongside technological advancements.¹⁴⁴

The examination above of both the revenge porn statutes and defamation law shows that neither approach, alone, can adequately address the concerns of AI-generated explicit content. The state statutes remain tethered to concepts of “reproduction” of original photographs and “reasonable expectation of privacy” that assume an original intimate moment was captured, which is entirely outside the realm of content created through AI machine learning and an algorithm.¹⁴⁵

While defamation law focuses on falsity which aligns conceptually with AI-generated content, there are still some procedural barriers in place. The one-year statutes of limitations under both the New York and New Jersey statutes, as well as the rejection of the discovery rule in defamation cases, potentially creates timing challenges for victims who may not immediately discover the explicit content.¹⁴⁶ As the court noted in *Firth v. State*, the single publication rule serves to reduce “the possibility of hardship to plaintiffs by allowing the collection of all damages in one case,” yet this benefit is undermined when victims cannot timely discover the publication.¹⁴⁷

The fairly recent passing of the TAKE IT DOWN Act represents a significant step toward addressing these gaps, but broader reforms remain necessary, especially as AI-technology only gets better.¹⁴⁸ An effective legal approach must address both criminal deterrence and swift content

¹⁴³ Warren & Brandeis, *supra* note 42, at 195.

¹⁴⁴ *Griswold*, 381 U.S. at 484; *Carpenter*, 585 U.S. at 338.

¹⁴⁵ N.J.S.A. § 2C:14-9; N.Y. Penal Law §245.15; *see supra* Part IV (discussing statutory construction limitations).

¹⁴⁶ *See supra* Part V (noting that both New York and New Jersey impose one-year limitations periods for defamation claims running from the date of publication rather than discovery).

¹⁴⁷ *Firth*, 98 N.Y.2d at 370.

¹⁴⁸ S. 4569, 118th Cong. (2024).

removal, as well as provide remedies that meaningfully compensate victims for the substantial psychological, professional, and social harms suffered when anonymous users hiding behind a computer screen generate explicit content through artificial intelligence.

The Taylor Swift incident highlights the massive dissemination potential of AI-generated explicit content and underscores the unfortunate reality of the perpetual existence of online content.¹⁴⁹ While the nudge of Swift's highly competent lawyers likely prompted rapid platform action, most victims of the 500 million individuals affected by this digital sexual abuse lack the financial resources and public profile necessary to mobilize such a speedy response.¹⁵⁰ As legal scholar Danielle Keats Citron argues, "sexual privacy sits at the apex of privacy values because of its importance to sexual agency, intimacy, and equality."¹⁵¹ Future state legislative and judicial developments must acknowledge and confront the unfortunate reality that AI-generated explicit content will only become more sophisticated with time. These future legislative and judicial actions must explicitly encompass AI-generated content and discovery challenges surrounding such content and must introduce language holding platforms accountable for the medium of disseminating such images, namely responsibility in identifying and removing AI-generated explicit content.

As technology continues to rapidly advance, statutes and regulations designed to protect individuals from its harms need to keep pace with it. The victim stories told in this article are not abstractions, but reminders of the human costs that lie behind the lag of the law.¹⁵² Thoughtful and strategic drafting of state and federal statutes, paired with accountability for the platforms that can

¹⁴⁹ See *supra* Part II (outlining the mass dissemination of explicit photographs of Swift).

¹⁵⁰ See *supra* Introduction (identifying the number of victims of revenge porn); see also *supra* Part II (demonstrating how fast platforms work to resolve the dissemination issue).

¹⁵¹ Citron, *supra* note 59, at 1874.

¹⁵² See *supra* Introduction (describing a case where a woman's ex-lover sent intimate images to her mother and business associates).

host this content can create robust protections against intimate image abuse and deepfake creation and dissemination.