Proskauer

Take it Down Act Signed into Law, Offering Tools to Fight Non-Consensual Intimate Images and Creating a New Image Takedown Mechanism

New Media and Technology Law Blog on **May 29, 2025**

- Law establishes national prohibition against nonconsensual online publication of intimate images of individuals, both authentic and computer-generated.
- First federal law regulating AI-generated content.
- Creates requirement that covered platforms promptly remove depictions upon receiving notice of their existence and a valid takedown request.
- For many online service providers, complying with the Take It Down Act's notice-and-takedown requirement may warrant revising their existing DMCA takedown notice provisions and processes.
- Another carve-out to CDA immunity? More like a dichotomy of sorts….

On May 19, 2025, President Trump signed the bipartisan-supported Take it Down Act into law. The law prohibits any person from using an "interactive computer service" to publish, or threaten to publish, nonconsensual intimate imagery (NCII), including AI-generated NCII (colloquially known as revenge pornography or deepfake revenge pornography). Additionally, the law requires that, within one year of enactment, social media companies and other covered platforms implement a notice-and-takedown mechanism that allows victims to report NCII. Platforms must then remove properly reported imagery (and any known identical copies) within 48 hours of receiving a compliant request.

Support for the Act and Concerns

The Take it Down Act attempts to fill a void in the policymaking space, as many states had not enacted legislation regulating sexual deepfakes when it was signed into law. The Act has been described as the first major federal law that addresses harm caused by AI. It passed the Senate in February of this year by unanimous consent and passed the House of Representatives in April by a vote of 409-2. It also drew the support of many leading technology companies.

Despite receiving almost unanimous support in Congress, some digital privacy advocates have expressed some concerns that the new notice-and-takedown mechanism could have some unintended consequences for digital privacy in general. For example, some commentators have suggested that the statute's takedown provision is written too broadly and lacks sufficient safeguards against frivolous requests, potentially leading to the removal of lawful content –especially given the short 48-hour time to act following a takedown request. [Note: In 2023, we similarly wrote about abuses of the takedown provision of the Digital Millennium Copyright Act]. In addition, some have argued that the law could undermine end-to-end encryption by possibly forcing such companies to "break" encryption to comply with the removal process. Supporters of the law have countered that private encrypted messages would likely not be considered "published" under the text of the statute (which uses the term "publish" as opposed to "distribute").

Criminalization of NCII Publication for Individuals

The Act makes it unlawful for any person "to use an interactive computer service to knowingly publish an intimate visual depiction of an identifiable individual" under certain circumstances.[1] It also prohibits threats involving the publishing of NCII and establishes various criminal penalties. Notably, the Act does not distinguish between authentic and AI-generated NCII in its penalties section if the content has been published. Furthermore, the Act expressly states that a victim's prior consent to the creation of the original image or its disclosure to another individual does not constitute consent for its publication.

New Notice-and-Takedown Requirement for "Covered Platforms"

Along with punishing individuals who publish NCII, the Take it Down Act requires covered platforms to create a notice-and-takedown process for NCII within one year of the law's passage. Below are the main points for platforms to consider:

- **Covered Platforms**. The Act defines a "covered platform" as a "website, online service, online application, or mobile application" that serves the public and either provides a forum for user-generated content (including messages, videos, images, games, and audio files) or regularly deals with NCII as part of its business.
- **Notice-and-Takedown Process**. Covered platforms must create a process through which victims of NCII (or someone authorized to act on their behalf) can send notice to them about the existence of such material (including a statement indicating a "good faith belief" that the intimate visual depiction of the individual is nonconsensual, along with information to assist in locating the unlawful image) and can request its removal.
- **Notice to Users**. Adding an additional compliance item to the checklist, the Act requires covered platforms to provide a "clear and conspicuous" notice of the Act's notice and removal process, such as through a conspicuous link to another web page or disclosure.
- **Removal of NCII**. Within 48 hours of receiving a valid removal request, covered platforms must remove the NCII and "make reasonable efforts to identify and remove any known identical copies."
- **Enforcement**. Compliance under this provision will be enforced by the Federal Trade Commission (FTC).
- **Safe Harbor**. Under the law, covered platforms will not be held liable for "good faith" removal of content that is claimed to be NCII "based on facts or circumstances from which the unlawful publishing of an intimate visual depiction is apparent," even if it is later determined that the removed content was lawfully published.

*Compliance Note***:** For many online service providers, complying with the Take It Down Act's notice-and-takedown requirement may warrant revising their existing DMCA takedown notice provisions and processes, especially if those processes have not been reviewed or updated for some time. Many "covered platforms" may rely on automated processes (or a combination of automated efforts combined with targeted human oversight) to fulfill Take It Down Act requests and meet the related obligation to make "reasonable efforts" to identify and remove known identical copies. This may involve using tools for processing notices, removing content and detecting duplicates. As a result, some providers should consider whether their existing takedown provisions should also be amended to address these new requirements and how they will implement these new compliance items on the backend using the infrastructure already in place for the DMCA.

What about CDA Section 230?

Section 230 of the Communications Decency Act ("CDA"), 47 U.S.C § 230, prohibits a "provider or user of an interactive computer service" from being held responsible "as the publisher or speaker of any information provided by another information content provider." Courts have construed the immunity provisions in Section 230 broadly in a variety of cases arising from the publication of user-generated content.

Following enactment of the Take It Down Act, some important questions for platforms are: (1) whether Section 230 still protects platforms from actions related to the hosting or removal of NCII; and (2) whether FTC enforcement of the Take It Down Act's platform notice-and-takedown process is blocked or limited by CDA immunity.

On first blush, it might seem that the CDA would restrict enforcement against online providers in this area, as decisions regarding the hosting and removal of third party content would necessarily treat a covered platform as a "publisher or speaker" of third party content. However, a deeper examination of the text of the CDA suggests the answer is more nuanced.

It should be noted that the Good Samaritan provision of the CDA (47 U.S.C § 230(c)(2)) could be used by online providers as a shield from liability for actions taken to proactively filter or remove third party NCII content or remove NCII at the direction of a user's notice under the Take It Down Act, as CDA immunity extends to good faith actions to restrict access to or availability of material that the provider or user considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Moreover, the Take It Down Act adds its own safe harbor for online providers for "good faith disabling of access to, or removal of, material claimed to be a nonconsensual intimate visual depiction based on facts or circumstances from which the unlawful publishing of an intimate visual depiction is apparent, regardless of whether the intimate visual depiction is ultimately determined to be unlawful or not."

Still, further questions about the reach of the CDA prove more intriguing. The Take It Down Act appears to create a dichotomy of sorts regarding CDA immunity in the context of NCII removal claims. Under the text of the CDA, it appears that immunity would not limit FTC enforcement of the Take It Down Act's notice-and-takedown provision affecting "covered platforms." To explore this issue, it's important to examine the CDA's exceptions, specifically 47 U.S.C § 230(e)(1).

Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title [i.e., the Communications Act], chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

Under the text of the CDA's exception, Congress carved out Section 223 and 231 of the Communications Act from the CDA's scope of immunity. Since the Take It Down Act states that it will be codified at Section 223 of the Communications Act of 1934 (i.e., 47 U.S.C. 223(h)), it appears that platforms would not enjoy CDA protection from FTC civil enforcement actions based on the agency's authority to enforce the Act's requirements that covered platforms "reasonably comply" with the new Take It Down Act notice-and-takedown obligations.

However, that is not the end of the analysis for platforms. Interestingly, it would appear that platforms would generally still retain CDA protection (subject to any exceptions) from claims related to the hosting or publishing third party NCII that have not been the subject of a Take It Down Act notice, since the Act's requirements for removal of NCII by platforms would not be implicated without a valid removal request.[2] Similarly, a platform could make a strong argument that it retains CDA immunity from any claims brought by an individual (rather than the FTC) for failing to reasonably comply with a Take It Down Act notice. That said, it is conceivable that litigants – or event state attorneys general – might attempt to frame such legal actions under consumer protection statutes, as the Take It Down Act states that a failure to reasonably comply with an NCII takedown request is an unfair or deceptive trade practice under the FTC Act. Even in such a case, platforms would likely contend that such claims by these non-FTC parties are merely claims based on a platform's role as publisher of third party content and are therefore barred by the CDA.

Ultimately, most, if not all, platforms will likely make best efforts to reasonably comply with the Take It Down Act, thus avoiding the above contingencies. Yet, for platforms using automated systems to process takedown requests, unintended errors may occur and it's important to understand how and when the CDA would still protect platforms against any related claims.

Looking Ahead

It will be up to a year before the notice-and-takedown requirements become effective, so we will have to wait and see how well the process works in eradicating revenge pornography material and intimate AI deepfakes from platforms, how the Act potentially affects messaging platforms, how aggressively the Department of Justice will prosecute offenders, and how closely the FTC will be monitoring online platforms' compliance with the new takedown requirements.

It also remains to be seen whether Congress has an appetite to pass more AI legislation. Less than two weeks before the Take it Down Act was signed into law, the Senate Committee on Commerce, Science, and Transportation held a hearing on "Winning the AI Race" that featured the CEOs of many well-known AI companies. During the hearing, there was bipartisan agreement on the importance of sustaining America's leadership in AI, expanding the AI supply chain and not burdening AI developers with a regulatory framework as strict as the EU AI Act. The senators listened to testimony from tech executives calling for enhanced educational initiatives and the improvement of infrastructure needed for advancing AI innovation, alongside discussing proposed bills regulating the industry, but it was not clear whether any of these potential policy solutions would receive enough support to be signed into law.

The authors would like to thank Aniket C. Mukherji, a Proskauer legal assistant, for his contributions to this post.

---

[1] The Act provides that the publication of the NCII of an adult is unlawful if (for authentic content) “the intimate visual depiction was obtained or created under circumstances in which the person knew or reasonably should have known the identifiable individual had a reasonable expectation of privacy,” if (for AI-generated content) “the digital forgery was published without the consent of the identifiable individual,” and if (for both authentic and AI-generated content) what is depicted “was not voluntarily exposed by the identifiable individual in a public or commercial setting,” “is not a matter of public concern,” and is intended to cause harm or does cause harm to the identifiable individual. The publication of NCII (whether authentic or AI-generated) of a minor is unlawful if it is published with intent to “abuse, humiliate, harass, or degrade the minor” or “arouse or gratify the sexual desire of any person.” The Act also lists some basic exceptions, such as publications of covered imagery for law enforcement investigations, legal proceedings, or educational purposes, among other things.

[2] Under the Act, “Upon receiving a valid removal request from an identifiable individual (or an authorized person acting on behalf of such individual) using the process described in paragraph (1)(A)(ii), a covered platform shall, as soon as possible, but not later than 48 hours after receiving such request—

(A) remove the intimate visual depiction; and

(B) make reasonable efforts to identify and remove any known identical copies of such depiction.

View original.

Related Professionals

- **Jeffrey D. Neuburger**