Articles + Publications | June 9, 2025

Platforms Face Section 230 Shift From Take It Down Act

WRITTEN BY

Thomas J. Cunningham | Michael J. McMorrow

On May 19, President Donald Trump signed the Take It Down Act into law.[1] The act will have an immediate impact on platform providers, which will be required to actively monitor and, in many cases, censor the speech of their users.

The act criminalizes a variety of acts that constitute the nonconsensual publication of intimate and sexualized content in order to combat deepfake pornography.[2] It received strong bipartisan support.

In addition to the criminal penalties for individual wrongdoers, the act establishes a notice and removal regime that will require platform providers to monitor the content transmitted or published by their platforms and remove content that may violate the act.

Notice and Removal Provisions Threaten Self-Censorship

The civil provisions of the Take It Down Act are of more concern to platform and telecom companies. Section 3 of the act creates a notice and removal process that any covered platform must establish within the next year.

The term “covered platform” is very broad. It includes any “website, online service, online application, or mobile application” that “serves the public” and either “primarily provides a forum for user-generated content” or any services that regularly “publish, curate, host, or make available content of nonconsensual intimate visual depictions.”[3]

The term “covered platform” excludes broadband providers, email and any “online service, application, or website” that consists primarily of content preselected by the provider of the service, and for which any interactive functionality like chat or comments is incidental, dependent upon, or directly related to the provision of the content.[4]

Although the obvious targets of this definition are large, public-facing social media platforms featuring user-generated content such as Facebook, YouTube, X and Instagram, the exclusions leave many types of platforms for private communication open to liability.

Messaging platforms remain subject to the notice and takedown provisions, as do cloud computing and storage platforms.

The Take It Down Act requires each covered platform to first establish a process where an individual — or an "authorized person" acting "on behalf of such individual" — may notify the platform of an intimate visual depiction and a "good faith belief that any intimate visual depiction … is not consensual," and can request immediate removal.

Second, each covered platform must provide a "clear and conspicuous notice" of the procedures to invoke the process for notice and removal. Once the process is invoked, the platform must remove any intimate visual depiction and also "make reasonable efforts to identify and remove any known identical copies of such depiction" within 48 hours after receiving "a valid removal request."

The act does not define the term "authorized person acting on behalf of [an] individual." The bounds of this term will need to be construed by the courts or the Federal Trade Commission.

Any person can claim to be an authorized person under the act. What evidence of authorization the act requires is not discussed in the bill, and whether a takedown request is valid could be interpreted in any number of ways.

The term "identifiable individual," while defined in the act to mean an individual "whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with [an] intimate visual depiction,"[5] raises further questions of what level of certainty a platform would need to determine that the individual is identified.

A blurry photograph, a partial tattoo or birthmark, a face concealed in shadows, and countless other iterations of questionable identity all could cause confusion as to whether an individual is identifiable. An individual determination of the identity for each allegedly offending visual depiction will likely be required unless the FTC engages in rulemaking to clarify the term.

The notice and takedown provisions apply to a broader swath of content than do the criminal provisions of the act.

The criminal provisions apply only to intimate visual depictions that are published without consent of the depicted individual, and also involve a "reasonable expectation of privacy," outside of any "public or commercial setting," that is "not a matter of public concern" and is intended to, or does, "cause harm."[6]

The notice and takedown provisions, on the other hand, require only an intimate visual depiction that "includes a depiction of the identifiable individual" and "was published without the consent of the identifiable individual" to trigger an obligation to act.[7] The notice and takedown provisions notably do not require that the intimate visual depiction be of the identifiable individual, only that the identifiable individual be depicted in some way.

Although the act limits the scope of the term "intimate visual description" to the meaning given in the 2022 Consolidated Appropriations Act,[8] it is doubtful that attempts to enforce the act will be limited to pornographic images.

In a recent address to a joint session of Congress, the president expressed a desire to use the Take It Down Act on his own behalf, stating, "[T]hank you to John Thune and the Senate. A great job. To criminalize the publication of such images online. This terrible, terrible thing. And once it passes the House, I look forward to signing that bill into law. Thank you. And I'm going to use that bill for myself too."[9]

The act's notice and takedown provisions are designed to encourage mass takedown requests, vague requests and requests from people other than the identified party.

Coupled with the act's provision requiring a covered platform to determine the validity of the request and remove both the intimate visual depiction and any copies of it within 48 hours, most platforms, particularly smaller platforms, will lack the ability to investigate the validity of the requests.

As discussed below, platforms are immunized when they remove the material in question, but not when they refuse to remove the material. All incentives will be to simply take material down upon request, without investigation, through the use of automated content detection filters and similar programs.

Effect of the Take It Down Act on Section 230 Immunity

The Take It Down Act changes the broad protections provided by Section 230 of the Communications Decency Act,[10] in ways that directly affect platform providers. Section 230, long considered the legal backbone of the internet, was passed to "promote the free exchange of information over the internet and encourage voluntary monitoring of offensive material."[11]

In doing so, Congress sought to immunize internet service providers from liability related to the content they host in order to avoid imposing content moderation duties on service providers.[12] Courts have interpreted Section 230 to establish broad federal immunity to actions that would make service providers liable for content originating from third-party users of a service.[13]

In passing Section 230, Congress was aware that the "specter of tort liability" within the "staggering" quantity of "information communicated via interactive computer services" would "have an obvious chilling effect."[14] Congress "considered the weight of the speech interests implicated and chose to immunize service providers to avoid [the] restrictive effect" that would occur if platforms chose to "restrict the number and type of messages posted" in the face of such potential liability.[15]

Courts have regularly found that "immunity from liability exists for '(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.'"[16]

The broad immunity provided by Section 230 has protected social media companies, VoIP platforms, search engines, online marketplaces, and many others from liability derived from content they had no role in creating. Section 230 eliminates any duty on the part of a platform provider to monitor and censor the content of communications made by third parties using the platform.

Two other, less publicized purposes of Section 230 were to "encourage the development of technologies which

maximize user control over what information is received by individuals," and to "remove disincentives for the development and utilization of blocking and filtering technologies."[17]

To that end, Section 230 also immunizes platforms against "any action voluntarily taken in good faith 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."[18]

The Take It Down Act introduces a new restriction on those immunities. The act includes a safe harbor for a platform's "good faith disabling of access to, or removal of, material claimed to be a nonconsensual intimate visual depiction."[19] This safe harbor mimics the immunity provided for actions taken to "restrict access to or availability of material" in the Communications Decency Act.

The act provides no safe harbor, however, for rejecting or refusing to honor a request for removal, whether from an identified individual or from an authorized person. Any "failure to reasonably comply with the notice and takedown obligations … shall be treated as a violation of a rule" under Section 18(a)(1)(B) of the FTC Act.[20]

The Take It Down Act contains no guardrails against false, frivolous or bad faith requests, requiring only that an authorized person have a good faith belief that consent is lacking.

End-to-end encrypted messaging platforms, including the popular platforms Signal, Telegram, WhatsApp, Facebook Messenger and others, will face additional concerns. Those platforms, due to the encryption of messages, will have a legal requirement to remove content that they will have no ability to access or even identify, short of breaking the encryption on which their users rely.

Considering the vagueness of the terms "authorized person," "good faith belief," and "identifiable individual," and combining that vagueness with the sizeable penalties authorized for violation of a rule under the FTC Act — currently $53,088.00 per violation[21] — any business could understandably err on the side of taking down the material in question, even if the business has concerns over the identity of the individual or the validity of the authorization of an authorized person. No liability can attach from taking the material down, while liability can attach from leaving the material in place.

More important than the limits of the Take It Down Act's definitions, however, is the fact that the act contradicts the basic immunity provided by Section 230(c)(1) of the Communications Decency Act, that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

The act treats the providers or users of interactive computer services in exactly that way, by imposing liability on them as the publisher or speaker of "information provided by another information content provider." It is expected to have the "obvious chilling effect" that Congress originally sought to avoid by passing Section 230.

---

[1] The text of the enrolled bill is available at https://www.congress.gov/bill/119th-congress/senate-bill/146/text?s=1&r=1&q=%7B%22search%22%3A%22%5C%22take+it+down%5C%22%22%7D.

[2] The Act makes it a criminal offense for any person to "use an interactive computer service to ?knowingly

publish any “intimate visual depiction of an identifiable individual” or any “digital ?forgery of an identifiable individual” in a variety of circumstances. Common to all those ?circumstances are that the depiction or forgery involve (a) an expectation of privacy by the ?identifiable individual; (b) involuntary disclosure; (c) not a matter of public concern; and (d) harm ?or intent to cause harm by publication. If the identifiable individual is a minor, the circumstances ?are broader, including any intent to “abuse, humiliate, harass, or degrade the minor” or to “arouse ?or gratify the sexual desire of any person.”

[3] Act, §4(3).

[4] Id., §4(3)(B).

[5] Id., §2(a)(2) (adding definitions to Section 223 of the Communications Act of 1934).

[6] Act, §2(a)(2)(A).

[7] Id., §3(a)(1)(A)

[8] See Id., §2(e), referencing 15 U.S.C. § 6851(a)(5).

[9] American Presidency Project, March 4, 2025 Address to Joint Session of Congress, (https://www.presidency.ucsb.edu/documents/address-before-joint-session-the-congress-4).

[10] 47 U.S.C. §230(c)(1), (c)(2).

[11] *Carafano v. Metrosplash.com Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003)?.

[12] Id. at 1123-24?.

[13] See *Perfect 10 Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007)?.

[14] *Zeran v. Am. Online Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).?

[15] Id.

[16] *United States v. Stratics Networks Inc.*, 721 F. Supp. 3d 1080, 1103 (S.D. Cal. 2024), citing ?*Barnes v. Yahoo! Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009).?

[17] 47 U.S.C. §230(b)(3), (b)(4).

[18] 47 U.S.C. §230(c)(2)(A).

[19] See S. 146, § 3(a)(4).?

[20] ?15 U.S.C. 57a(a)(1)(B)?.

[21] This number is adjusted for inflation every year. See FR Doc. 2025-01361 (Jan. 16, 2025).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber