Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

The TAKE IT DOWN Act: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images

May 20, 2025

On April 28, 2025, Congress passed S. 146, the TAKE IT DOWN Act, a bill that criminalizes the nonconsensual publication of intimate images, including "digital forgeries" (i.e., deepfakes), in certain circumstances. It also requires certain websites and online or mobile applications, identified as "covered platforms," to implement a "notice-and-removal" process to remove such images at the depicted individual's request. The President signed the bill into law on May 19, 2025. The bill's criminal prohibition takes effect immediately, while covered platforms have one year (until May 19, 2026) to establish the required notice-and-removal process. This Legal Sidebar provides an overview of laws prohibiting the nonconsensual distribution of intimate images, describes the major provisions of the TAKE IT DOWN Act, and analyzes legal questions that may be posed by regulated individuals and entities, Congress, and the courts.

Laws Addressing the Nonconsensual Distribution of Intimate Images

Over the last 12 years, states have adopted a range of laws specifically addressing the nonconsensual distribution of intimate images, sometimes referred to as "nonconsensual pornography" or "revenge porn." In 2022, Congress passed a law establishing a federal civil right of action for victims of nonconsensual pornography as part of its reauthorization of the Violence Against Women Act (VAWA). The law generally authorizes depicted individuals to sue the disclosing party in federal court for money damages or injunctive relief. While some jurisdictions (e.g., New York) expressly include digitally created or altered images in their nonconsensual pornography laws, the federal civil action, as originally enacted, does not explicitly address such images. As a result, it is not settled whether VAWA's right of action encompasses such digitally modified depictions. Some Members of Congress introduced bills in the 118th and 119th Congresses to expand the existing cause of action or create a parallel cause of action for images created or altered using artificial intelligence (AI) or other digital technologies.

Congressional Research Service
https://crsreports.congress.gov
LSB11314

The TAKE IT DOWN Act

The TAKE IT DOWN Act (the Act), which stands for "Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act," makes two main changes to federal law. First, the Act amends Section 223 of the Communications Act of 1934 (47 U.S.C. § 223) to add new criminal prohibitions related to the publication of intimate images. Second, the Act creates new requirements for covered platforms that the Federal Trade Commission (FTC) would enforce.

Criminal Prohibitions

The Act makes it unlawful in certain circumstances for any person to "use an interactive computer service"—an existing term broadly construed to cover most online applications and services—to "knowingly publish" either an "intimate visual depiction" or a "digital forgery" of an identifiable individual. The terms "knowingly" and "publish" are not defined in the Act or the statute that it amends. The term "intimate visual depiction" is defined by reference to the existing federal right of action and includes a visual depiction of an identifiable individual engaged in "sexually explicit conduct." A "digital forgery" under the TAKE IT DOWN Act is an intimate visual depiction of an identifiable individual created or altered using AI or other technological means. The Act defines "identifiable individual" as someone "who appears in whole or in part in an intimate visual depiction" and "whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with such intimate visual depiction."

The criminal prohibitions consist of seven separate offenses: (1) publications involving "authentic" intimate visual depictions of adults; (2) publications involving authentic visual depictions of minors (under 18); (3) publications involving digital forgeries of adults; (4) publications involving digital forgeries of minors; (5) threats involving authentic intimate depictions of adults or minors; (6) threats involving digital forgeries of adults; and (7) threats involving digital forgeries of minors. As these are criminal offenses, the government bears the burden of proving each element beyond a reasonable doubt.

For the publication-related offenses involving depictions of adults, the government must show that, in addition to knowingly publishing the material, the defendant intended the publication to cause harm, or that the publication did cause the identifiable individual harm, "including psychological, financial, or reputational harm." The offenses involving depictions of adults also contain elements regarding consent and content:

- that an authentic 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," or, in the case of a digital forgery, the material was published without the identifiable individual's consent;
- that "what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting"; and
- that "what is depicted is not a matter of public concern."

The "public concern" element appears to refer to a First Amendment concept. The Supreme Court has held that "[s]peech deals with matters of public concern when it can 'be fairly considered as relating to any matter of political, social, or other concern to the community,' or when it 'is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public,'" regardless of its "arguably 'inappropriate or controversial character.'" In the context of a First Amendment analysis, speech about matters of public concern is generally entitled to greater protection than speech about purely private matters.

The publication offenses involving depictions of minors do not have the same consent and content elements. Criminal liability attaches if the defendant knowingly publishes the depictions and intends to "abuse, humiliate, harass or degrade the minor" or "arouse or gratify the sexual desire of any person."

The Act contains exceptions for certain types of publications, including good-faith disclosures to law enforcement or "for a legitimate medical, scientific, or education purpose." It is not an offense for a person to possess or publish an intimate visual depiction or digital forgery of "himself or herself engaged in nudity or sexually explicit conduct." Material that violates specified child exploitation laws is also excluded from the criminal prohibition.

In addition, the Act makes it unlawful to "intentionally threate[n]" to commit one of the publication-related offenses "for the purpose of intimidation, coercion, extortion, or to create mental distress."

A person who violates one of the publication offenses pertaining to depictions of adults is subject to criminal fines, imprisonment of up to two years, or both. The penalties for publishing depictions of minors are greater, with potential imprisonment of up to three years. Threats to publish authentic visual depictions carry the same penalties as the applicable publication offenses: fines and up to two years' imprisonment for threatening to publish a depiction of an adult and up to three years' imprisonment for a depiction of a minor. The potential term of imprisonment for threat-related offenses involving digital forgeries is not more than 18 months, or 30 months for threats involving minors. The Act also prescribes forfeiture of material distributed in violation of a publication-related offense as well as property used to commit the violation or obtained as a result of the violation.

Notice-and-Removal Requirements

The Act requires a covered platform to establish a specified notice-and-removal process by May 19, 2026. A covered platform is "a website, online service, online application, or mobile application" (website or app) that serves the public and either "primarily provides a forum for user-generated content" or publishes, curates, hosts, or makes available content of nonconsensual intimate visual depictions in the regular course of trade or business. A covered platform does not include the following: (1) a provider of broadband internet access service; (2) email; (3) a website or app that "consists primarily of content that is not user generated but is preselected by the provider" and "for which any chat, comment, or interactive functionality is incidental to, directly related to, or dependent on the provision of" that preselected content. The last exclusion does not apply to websites or apps in the business of publishing or hosting nonconsensual intimate visual depictions.

Under the Act, a covered platform must establish a process that allows an identifiable individual or their authorized representative to notify the platform and seek removal of an intimate visual depiction of that individual published without the individual's consent. The notification must be in writing and include "an identification of, and information reasonably sufficient for the covered platform to locate," the depiction; "a brief statement" of the individual's "good faith belief" that the published depiction "is not consensual," including any relevant information for the covered platform to verify the lack of consent; and the signature of and contact information for the identifiable individual or their representative. Upon receiving such a notice, a covered platform must remove the intimate visual depiction "as soon as possible" but no later than 48 hours after receiving the notice. Within that time frame, the platform must also "make reasonable efforts to identify and remove any known identical copies of such depiction." A covered platform must provide a "plain language" explanation of its notice-and-removal process on its site. The Act provides that a covered platform "shall not be liable for any claim based on" its "good faith disabling of access to, or removal of" a depiction based on an "apparent" unlawful publication, even if the depiction turns out to be lawful.

The Act authorizes the FTC to enforce the notice-and-removal requirements, stating that a "failure to reasonably comply with" these obligations constitutes "a violation of a rule defining an unfair or

deceptive act or practice" (UDAP violation) under the Federal Trade Commission Act (15 U.S.C. § 57a(a)(1)(B)). The Act extends the FTC's jurisdiction in this regard to nonprofit organizations, which are not usually covered by the FTC Act.

Legal Considerations for Congress

As with any new statute, the TAKE IT DOWN Act may be interpreted by a range of stakeholders from federal agencies (e.g., the Department of Justice, FTC), to regulated entities (e.g., covered platforms), to individuals the law was designed to protect (e.g., victims of nonconsensual pornography), some of whom may disagree about the meaning or scope of certain provisions. One interpretive question that might arise is what it means to "publish" an intimate visual depiction. If a court is asked to decide this question, it may look to the ordinary meaning of *publish*, because the term is not defined for purposes of the Act. *Merriam-Webster*, for example, defines *publish* as "to make generally known" or, as one court observed, "to disseminate to the public." A court applying this definition in the context of the TAKE IT DOWN Act could conclude that a person does not "publish" an intimate depiction by sending it to one other person through an email or direct message, even if the person used an interactive computer service. At least one federal court, however, has construed publishing activity more broadly to include what was then Twitter's direct messaging capabilities. That case involved a different section of the Communications Act, and an appellate court affirmed the decision on different grounds. If a court were to conclude that "publish" is ambiguous in the context of the Act, it might apply the "rule of lenity," a judicial principle "that ambiguities about the breadth of a criminal statute should be resolved in the defendant's favor."

The TAKE IT DOWN Act does not amend VAWA, but courts may nevertheless consider the Act relevant to deciding whether VAWA's federal civil right of action applies to digital forgeries. The TAKE IT DOWN Act creates separate offenses for publications involving "intimate visual depictions" and "digital forgeries"—a distinction that Congress did not replicate in the notice-and-removal provisions or in VAWA. Courts generally presume that Congress uses terms consistently within the same act. When Congress uses different terms, courts usually refrain from "'ascribing to one word a meaning so broad' that it assumes the same meaning as another statutory term." Thus, a reviewing court might reason, on one hand, that by using two different terms in the criminal provisions of the TAKE IT DOWN Act, Congress meant to cover two distinct types of material. Following that reasoning, the notice-and-removal provisions, which mention only "intimate visual depictions," might not apply to digital forgeries. Based on the same premise, a court could conclude that by not amending VAWA to include digital forgeries, Congress intended to reserve VAWA's private right of action for persons whose actual intimate images were disclosed without their consent. On the other hand, the definitions in the TAKE IT DOWN Act suggest that the terms "intimate visual depiction" and "digital forgery" overlap. The term "intimate visual depiction," which is defined by reference to VAWA, may be broad enough, standing alone, to include digitally created or altered images. The TAKE IT DOWN Act defines "digital forgery" as an "intimate visual depiction" created through technological means, suggesting that a digital forgery is a type of intimate visual depiction. That reading is potentially reinforced by the titles of the offenses, which include the term "authentic" before intimate visual depictions, potentially to distinguish actual depictions from digital forgeries. Based on the statutory context, then, a court might conclude that intimate visual depictions can include authentic images and digital forgeries when used in the notice-and-removal provisions and in VAWA.

Another consideration might be the scope of potential liability—civil and criminal—for online platforms if they publish or decline to remove third-party content that qualifies as a proscribed intimate visual depiction or digital forgery. Interactive computer services are immunized from certain types of liability for merely hosting third-party content pursuant to Section 230 of the Communications Act of 1934 (47 U.S.C. § 230). Some providers have raised Section 230 as a defense to FTC claims alleging UDAP violations, with varying degrees of success. The TAKE IT DOWN Act does not expressly address the

relationship between its notice-and-removal requirements (backed by UDAP penalties) and Section 230, though it provides that a "covered platform shall not be liable for any claim based on the covered platform's good faith disabling of access to, or removal of, material claimed to be a nonconsensual intimate visual depiction" in certain circumstances. If the FTC were to bring a UDAP action against an interactive computer service provider, that provider might seek to dismiss the claim on Section 230 grounds, arguing that the TAKE IT DOWN Act leaves Section 230's immunity provision intact. The FTC might argue in response that the TAKE IT DOWN Act implicitly repeals Section 230 for UDAP violations under the Act, a question that a court may resolve as a matter of statutory interpretation by considering, among other factors, whether the two sets of provisions can be harmonized in a way that gives effect to each.

Unlike most types of civil claims, federal criminal law is expressly excluded from Section 230 protection. Accordingly, Section 230 itself would not immunize interactive computer service providers from criminal liability under the TAKE IT DOWN Act. Still, the TAKE IT DOWN Act provides a defense if a person "solely . . . provid[ed] access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication." This defense, which Congress passed in 1996 as part of the Communications Decency Act, does not apply to "conspirator[s]" or persons who, in addition to providing access or connection, own or control the facility, system, or network that "engaged in the violation." Few courts have interpreted the defense's scope, particularly in the context of today's online infrastructure. How it might apply, for example, to social media companies, internet access providers, online marketplaces, search engines, or app stores remains to be seen. Based on its text, the defense to criminal liability does not appear to be co-extensive with Section 230 protection, which turns, in part, on whether an interactive computer service provider is the "information content provider," meaning "responsible, in whole or in part, for the creation or development of" the allegedly offending material. The TAKE IT DOWN Act's criminal defense, by comparison, seems to turn on whether the provider owns or controls a website or app where a prohibited depiction was published. Even in the absence of a defense, in a criminal trial the government would still need to prove, among other elements, that the provider published a prohibited depiction "knowingly." The *mens rea* (i.e., mental state) *knowingly* typically requires evidence of actual, subjective awareness of the nature of the material, but courts have also considered evidence of "willful blindness" in some circumstances.

Because the TAKE IT DOWN Act regulates speech in the form of visual depictions, First Amendment questions may be at the forefront of any legal challenges. In particular, because the Act regulates speech on the basis of its content (i.e., sexually explicit depictions), it could receive the most rigorous form of First Amendment scrutiny (strict scrutiny) if challenged in court. Under that standard, the government would need to show that the law is the least restrictive means of advancing a compelling governmental interest. In the event of a free-speech challenge to the Act's criminal prohibitions, a reviewing court might consider judicial decisions resolving First Amendment challenges to similar state nonconsensual pornography laws. The highest courts of six states (IL, IN, MN, NE, TX, and VT) have upheld their states' nonconsensual pornography laws against free-speech challenges, though one court did so in a nonprecedential (i.e., nonbinding) opinion. (As of the date of this writing, there were no reported judicial decisions analyzing free-speech defenses to claims brought under the federal VAWA right of action.) The criminal prohibitions in the TAKE IT DOWN Act share some of the features of the state laws upheld in those jurisdictions (most of which applied strict scrutiny), including rigorous mental state requirements (knowingly or specific intent), a focus on depictions of identifiable individuals, and exceptions for circumstances where a depicted adult does not have a reasonable expectation of privacy or the depiction is a matter of public concern. Where the TAKE IT DOWN Act primarily differs from those laws is its notice-and-removal requirements. While a range of individuals and organizations, including some regulated providers, expressed support for the legislation, some stakeholder groups have argued that the

notice-and-removal provisions are overbroad. They argue that platforms may be asked to remove lawful content, with no avenue for the user who posted the image to challenge a platform's good-faith decision. In the event of a lawsuit challenging the notice-and-removal requirements, a court's review of those provisions may be informed by decisions in other pending legal challenges, such as those involving state social media laws.

Author Information

Victoria L. Killion
Legislative Attorney

Disclaimer