

## CLIENT ALERT

# Congress Passes Take It Down Act, Imposing New Burdens on Platforms to Establish a Takedown Process for Nonconsensual Intimate Images

May 19, 2025

### AUTHORS

Nicholas Reddick | Susan Rohol | Elodie Currier Stoffel

The President signed into law today the Take It Down<sup>1</sup> Act, imposing new burdens on websites, forums, and other online platforms to address deepfake pornography and other forms of nonconsensual intimate imagery. The Act, which passed Congress nearly unanimously, gives websites who host user-generated content<sup>2</sup> one year to develop a notice and takedown process for nonconsensual digital forgeries of identifiable individuals.<sup>3</sup> When enacted, the Take It Down Act will cover a wide array of platforms across the internet, requiring their owners to draft new notices and develop new processes to comply.

<sup>1</sup> Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks ("Take It Down") Act, S. 146, 119<sup>th</sup> Cong. (2025) (hereinafter, "Take It Down Act").

<sup>2</sup> See Take It Down Act, Section 4(3). As discussed in detail later in this client alert, there are narrow exceptions to this definition.

<sup>3</sup> Take It Down Act, Section 3(a).

## The Problem: Deepfake Pornography and Nonconsensual Intimate Imagery

Deepfake pornography—or the use of software to create realistic nude images of unwilling participants—has been an issue for platforms for nearly a decade. The explosion of generative artificial intelligence/machine learning (“AI/ML”) software over the past three years, however, has raised the prevalence of these acts and profile of the issue. Current deepfakes are essentially indistinguishable from real-world content,<sup>4</sup> and making them is simple and near-costless. Nonconsensual intimate imagery produced using generative AI has been used to target celebrities, and government figures, but also as a day-to-day tool of harassment in middle and high schools.<sup>5</sup>

Deepfake pornography has also drawn attention to the broader issue of nonconsensual intimate media. Nonconsensual intimate media includes a wide array of content, including deepfake pornography, intimate image abuse by former partners (“revenge porn”) and digital sex crimes (“upskirting,” “downblousing,” and the use of hidden cameras to capture nude and/or sexual images of unwitting subjects). The proliferation of mobile phone cameras and microcameras, as well as the rise of social media, has assisted criminals in creating, monetizing, and sharing these images. In 2017, a study by the Cyber Civil Rights Initiative found that one in 12 American social media users had nonconsensual intimate media of them shared online, and one in eight had been threatened with such sharing.<sup>6</sup> Criminalized in 49 states and the District of Columbia, the sharing of nonconsensual intimate media is often tied to attempts to extort its victims for money or further images.<sup>7</sup>

## Existing State and Federal Regulation of Deepfakes and Nonconsensual Intimate Imagery

Prior regulation of deepfake pornography has been largely state-dependent, or has relied on existing criminal prohibitions on Child Sexual Abuse Material (“CSAM”) and other nonconsensual intimate imagery.<sup>8</sup> Regulation of nonconsensual intimate imagery at the state level has focused on criminalizing the act of sharing itself, as Section 230 created a major barrier for platform liability for the spread of nonconsensual intimate media. AI/ML developers have put up guardrails to make it more difficult for users to prompt their models to produce nudity in general, and

---

<sup>4</sup> This has particularly concerned researchers and advocates combatting Child Sexual Abuse Material (“CSAM”) who have noted that “AI CSAM is visually indistinguishable from real CSAM, even for trained [] analysts.” Internet Watch Foundation, *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, IWF (July 2024) <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>.

<sup>5</sup> Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in Schools*, NY TIMES (Apr. 8, 2024) <https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html>.

<sup>6</sup> Dr. Asia E. Eaton, Dr. Holly Jacobs & Yanet Ruvalcaba, 2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration (Cyber Civil Rights Initiative, June 2017), avail. at <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>.

<sup>7</sup> As one example, a bar exam taker filed suit against the hotel she had stayed at during the exam, alleging that she received email with personal information and a link to a video posted to a pornographic site depicting her in the hotel’s shower, which threatened to further publicize the video if she did not send more intimate material or pay a monthly fee. Debra Cassens Weiss, *Law School Grad Sues Hotel for \$100M After Discovering She Was Secretly Videotaped in Shower*, ABA Journal (Dec. 6, 2018) [https://www.abajournal.com/news/article/law\\_school\\_grad\\_sues\\_hotel\\_for\\_100m\\_after\\_discovering\\_she\\_was\\_secretly\\_vide](https://www.abajournal.com/news/article/law_school_grad_sues_hotel_for_100m_after_discovering_she_was_secretly_vide).

<sup>8</sup> Forty-nine states and the District of Columbia have laws criminalizing nonconsensual intimate imagery. Niki Saenz, *Let’s Be Realistic: Crafting an Effective Legal Remedy for Victims of Deepfake Pornography*, 66 ARIZONA L. REV. 785, 802.

nonconsensual intimate imagery in particular. Many social media platforms have also taken steps to ban nonconsensual intimate imagery and digital nonconsensual intimate imagery as state laws have proliferated.

California has taken a leading position in legislating to target harms posed by AI/ML's proliferation, enacting three bills in 2024 aimed to "protect individuals from the misuse of digital content."<sup>9</sup> California SB 981 required social media platforms to establish a reporting mechanism for sexually explicit deepfakes, and to investigate and remove the content within thirty (30) days.<sup>10</sup> Other states have enacted specific provisions criminalizing digital nonconsensual intimate imagery, but few others have enacted legislation which require action by platforms.<sup>11</sup> Texas's 2023 law, SB 1361, is representative of these efforts: it criminalizes persons who produce and "distribute" deepfake pornography, but provides little explanation of behavior that could constitute "distribution." To the extent that Section 230 does not bar liability, platforms could theoretically be found criminally liable.

### The Take It Down Act

Given the growing consensus on the harms of nonconsensual intimate imagery in an era of AI/ML, it is not surprising that congressional support for a solution was almost unanimous. The Take It Down Act, supported by over 120 organizations and tech platforms, initially passed unanimously in the Senate before passing the House of Representatives with a vote of 409 in favor, 2 against.

The Act, introduced by Senator Ted Cruz of Texas and Amy Klobuchar of Minnesota, creates criminal penalties for the intentional disclosure of nonconsensual intimate visual depictions through interactive services, including what the bill terms "digital forgeries"<sup>12</sup> of identifiable individuals. Digital forgeries as defined by the Act include both AI-generated nonconsensual intimate imagery, and nonconsensual images created through traditional software, such as photo editing software. In addition to its criminal provisions, the Act places substantial burdens on covered platforms to implement a report and removal process for nonconsensual intimate media.

The Act is written broadly. It defines "intimate visual depiction" as any visual depiction of adult genitals, pubic area, anus, or female nipples, or identifiable individuals engaging in sexually explicit conduct. When intimate imagery qualifies as "nonconsensual" under the law varies depending on whether it is of an adult or a minor. Intimate visual depictions of adults qualify if (1) the depicted individual had a reasonable expectation of privacy; (2) the depiction was not voluntarily produced in a commercial setting; (3) the image is not a matter of public concern; and (4) the publication is intended to cause harm or causes harm.<sup>13</sup> Intimate visual depictions of minor need only be used to

---

<sup>9</sup> *Governor Newsom Signs Bills to Crack Down on Sexually Explicit Deepfakes & Require AI Watermarking*, CAL. GOVERNOR GAVIN NEWSOM (Sept. 19, 2024) <https://www.gov.ca.gov/2024/09/19/governor-newsom-signs-bills-to-crack-down-on-sexually-explicit-deepfakes-require-ai-watermarking/>.

<sup>10</sup> In some circumstances, the law allows for a limited extension of up to sixty (60) days. See Cal. Bus. & Profs. Code. § 22671(b-c).

<sup>11</sup> Saenz, *supra* note 8, at 805.

<sup>12</sup> The Act defines "digital forgery" as any "intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual."

<sup>13</sup> Take It Down Act, Section 2(A). For minors, the definition is broader.

abuse, humiliate, harass, or degrade the minor pictured, or to arouse or gratify any person, to fall within the scope of the Act.

The Act also uses an expansive definition of “covered platforms:” they are any “website, online service, online application, or mobile application . . . that serves the public and . . . that primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files; or for which it is the regular course of trade or business . . . to publish, curate, host, or make available content of nonconsensual intimate visual depictions.”<sup>14</sup> Unlike California’s deepfake law, Texas and Florida’s content moderation laws, and many state comprehensive privacy laws, there is no size or monthly active user threshold for application. There are exceptions for providers of broadband internet services” (removing also, replacing “email” with “internet”), internet providers, and websites that consist primarily of non-user-generated content that is preselected by the website provider and where interactive features are “incidental to, directly related to, or dependent on the provision of the website’s content.”<sup>15</sup>

Covered platforms must, no later than one year after enactment, “establish a process” for identifiable individuals or their agents to notify the platform of intimate visual depictions and submit a request for the covered platform to remove the depiction.<sup>16</sup> The Act dictates specific requirements for the request for removal, including the signature of the requestor, identification of the depiction, a description of the grounds under which the individual believes the publication of the depiction was nonconsensual, and contact information for the requestor.<sup>17</sup> The Act also adds to the notice burden placed on platforms, requiring a “clear and conspicuous notice” and removal process that “is easy to read and in plain language” and “provides information regarding the responsibilities of the covered platform . . . including” a description of how requests for removal can be submitted.<sup>18</sup>

Once a platform is notified, covered platforms must, no later than 48 hours after receiving a request, remove the intimate visual depiction and “make reasonable efforts to identify and remove known identical copies of such depiction.”<sup>19</sup> Failure to implement the notice and takedown process can be investigated by the Federal Trade Commission and treated as an unfair or deceptive act or practice.<sup>20</sup>

While lacking an explicit preemption clause, the Take It Down Act does include a limitation on liability which provides that covered platforms are not liable for any claim based on such takedowns, so long as the action is in good faith.<sup>21</sup>

---

<sup>14</sup> Take It Down Act, Section 4(3)(A).

<sup>15</sup> Take It Down Act, Section 4(3)(B).

<sup>16</sup> Take It Down Act, Section 3(a)(1).

<sup>17</sup> *Id.*, Section 3(a)(1)(B).

<sup>18</sup> Take It Down Act, Section 3(a)(2).

<sup>19</sup> Take It Down Act, Section 3(a)(3).

<sup>20</sup> Take It Down Act, Section 3(b); *see also* 15 U.S.C. 57a(a)(1)(B).

<sup>21</sup> Take It Down Act, Section 3(a)(4).

## Practical Challenges to Implementation

The Take It Down Act casts a much wider net than state comprehensive privacy laws,<sup>22</sup> Florida and Texas's content moderation laws,<sup>23</sup> and California's deepfake reporting requirements.<sup>24</sup> The wide scope captures a variety of sites, users, and applications that may not have previously prepared for content moderation or content takedown procedures, or developed nuanced legal notices for their users. The law covers nearly any platform that allows user-generated content, with narrow exceptions for traditional publishers. Further, the law addresses not only deepfakes, but requires takedown of all nonconsensual intimate media, incorporating a complex definition of nonconsensual intimate media that requires platforms to grapple with concepts like whether an image is a matter of public concern, whether content was produced for commercial purposes, and where an individual has a reasonable expectation of privacy, all within 48 hours.

Even large and legally sophisticated platforms will face implementation challenges: the Act's takedown timeline requires greater action by platforms on a far shorter timeline. For example, California's SB 981 requires acknowledging receipt of a user's report within 48 hours, providing a status update within seven (7) days, and concluding an investigation within thirty (30) days.<sup>25</sup> SB 981 requires action only on the *instance* of the image reported by a user, and requires action only on deepfake pornography. By contrast, the Take It Down Act requires platforms not only to take down the individual instance reported within 48 hours, but to "make reasonable efforts to identify and remove any known identical copies. . . ."<sup>26</sup>

Platforms should also be aware of the potential interaction of the Take It Down Act and state content moderation laws, such as Florida's SB 7072 and Texas's HB 20. SB 7072, which was the subject of litigation before the Supreme Court in *Moody v. NetChoice, LLC* and remains partially enjoined,<sup>27</sup> requires social media platforms of a certain size to provide detailed disclosures of the standards they use to engage in content takedowns. Presently enforceable portions of Florida SB 7072 also require that platforms give users the ability to download content for a specific period after it is taken down. Large social media platforms will have to consider the interaction between SB 7072's emphasis on the right of content creators to be free from arbitrary takedown, the Take It Down Act's rapid removal provision, and the removal and investigation process conceptualized in California SB 981. These interactions remain backstopped by criminal provisions like Texas's on the one hand, and the limitations on liability

---

<sup>22</sup> See, e.g., the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (limiting application to businesses that have gross annual revenues of over \$25 million; collect, sell, or process the personal information of 100,000 or more Californians per year; or earn more than 50% of their annual revenue from selling or sharing personal information).

<sup>23</sup> Florida S.B. 7072 (2021); Texas H.B. 20 (2021) (applicable only to social media platforms with a given revenue threshold or high number of MAUs); See also *NetChoice, LLC v. Moody*, Case No. 4:21-cv-0220, ECF No. 180 (limiting the scope of a prior preliminary injunction such that elements of S.B. 7072 are enforceable).

<sup>24</sup> See Cal. Bus. & Profs. Code § 22670(d) (defining "social media platform" by reference to Cal. Bus. & Profs. Code Section 22675); Cal. Bus. & Profs. Code. § 22675(d-e) (defining social media platform as an internet-based service or application that meets four specified criteria, including allowing users to conduct a public profile, interact socially, create a friends list, and post user-generated content).

<sup>25</sup> Cal. Bus. & Profs. Code. § 22671(b-c).

<sup>26</sup> Take It Down Act, Section 3(a)(3)(B).

<sup>27</sup> 144 S. Ct. 2383 (2024); see also *NetChoice, LLC v. Moody*, Case No. 4:21-cv-0220, ECF No. 182 (removing portions of the preliminary injunction enjoining SB 7072).

## Congress Passes Take It Down Act, Imposing New Burdens on Platforms to Establish a Takedown Process for Nonconsensual Intimate Images

in Section 230 and the Take It Down Act on the other. The chart below summarizes some of the similarities, differences, and areas of overlap in these laws.

	Take It Down Act	California SB 981	Texas SB 1361 (criminalizing deepfake pornography)	Florida SB 7072 (content moderation)
<b>Regulated Websites/ Platforms</b>	Any website or digital platform that provides a forum for user-generated content	Social media platforms as defined by California law (platforms which, among other requirements, allow users to create profiles and lists of friends)	No explicit statutory application to websites or platforms	Social media platforms that do business in Florida and have annual gross revenues in excess of \$100 million, or at least 100 million monthly individual platform participants globally
<b>Platform liability for knowingly aiding, facilitating, or abetting violative content?</b>	Yes, as a failure to comply with the notice and takedown process	No	Platforms could be considered “persons” liable for “distribution” of deepfake pornography	N/A
<b>Required Web Disclosures</b>	Clear and conspicuous notice discussing the platform’s notice and removal obligations for nonconsensual intimate imagery, including instructions for submitting removal requests	None explicitly required, but disclosures may be needed to the extent required to create a “reasonably accessible mechanism” for reporting	N/A	Among other required disclosures, the standards by which the Company determines what media and accounts are removed
<b>Takedown Timeline for Nonconsensual Intimate Imagery</b>	48 hours from time of report to remove the reported media, and to take reasonable steps to remove all copies of the reported media	48 hours to acknowledge the report and temporarily remove the image reported, 7 days to provide a status update, 30 days (with a potential extension to 60 days in some circumstances) to investigate and determine permanent removal	N/A	N/A
<b>Who Can Report?</b>	The person depicted in the nonconsensual intimate imagery or their authorized representative	California users, depicted in the nonconsensual intimate imagery, with an account on the platform	N/A	N/A
<b>Enforcement Authority/Risk</b>	Investigation and enforcement by the Federal Trade Commission as an unfair and deceptive trade practice	None specified, but likely enforceable by the State Attorney General and/or local District Attorneys	Criminal prosecution	Investigation by the Florida Attorney General for unfair and deceptive trade practices. Penalties of up to \$10,000 per violation, or \$15,000 for certain protected groups
<b>Limitation on Liability for Removing Alleged Nonconsensual Intimate Imagery?</b>	Yes	No	N/A	No

As the chart above demonstrates, the Take It Down Act applies to more websites, allows for reports by a larger class of users, and requires more action by platforms on a shorter timeline and wider range of content than what is

## Congress Passes Take It Down Act, Imposing New Burdens on Platforms to Establish a Takedown Process for Nonconsensual Intimate Images

required under California law. This enhanced burden is not only applicable to social media companies, but to any platform that facilitates the exchange of user-generated content, regardless of size or revenues.

Platforms and websites have a year before they are required to have their report and takedown process established, and in the meantime, legal challenges remain possible. The Cyber Civil Rights Initiative and Electronic Frontier Foundation have criticized what they see as overbreadth, vagueness, and the burden the law may place on First Amendment protected content.<sup>28</sup> Regardless of these challenges, the Take It Down Act is sure to create new complexities and operational challenges for platforms and for companies with digital presences.

**If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.**

**Nicholas Reddick**

415 858 7595

[nreddick@willkie.com](mailto:nreddick@willkie.com)

**Susan Rohol**

310 855 3172

[srohol@willkie.com](mailto:srohol@willkie.com)

**Elodie Currier Stoffel**

212 728 3606

[ecurrier@willkie.com](mailto:ecurrier@willkie.com)

# WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HOUSTON LONDON LOS ANGELES MILAN  
MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Copyright © 2025 Willkie Farr & Gallagher LLP. All rights reserved.

This alert is provided for educational and informational purposes only and is not intended and should not be construed as legal advice, and it does not establish an attorney-client relationship in any form. This alert may be considered advertising under applicable state laws. Our website is: [www.willkie.com](http://www.willkie.com).

---

<sup>28</sup> See, e.g., Jason Kelly, *Congress Passes TAKE IT DOWN Act Despite Major Flaws*, ELEC. FRONTIER FOUND. (Apr. 28, 2025), <https://www.eff.org/deeplinks/2025/04/congress-passes-take-it-down-act-despite-major-flaws>.