TAKE IT DOWN Act Signed into Law by President Trump

June 15, 2025

Pittsburgh, PA

TEQ Magazine

(by **Kristen Petrina**)

On May 19, 2025, President Trump signed into the law the “TAKE IT DOWN Act (the “Act”). The Act includes data privacy, digital protections, and AI governance requirements of companies to remove deepfakes from “covered platforms”, particularly with a focus on nonconsensual intimate imagery (“NCII”).

The Act, whose acronym stands for “Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act” includes both criminal and civil elements; however, it does not create a new private right of action, rather provides the Federal Trade Commission with the enforcement authority over failures to comply with the notice and removal obligations, which would constitute an unfair or deceptive act or practice under the Federal Trade Commission Act.

Criminal and Civil Liability

The Act criminalizes the publication of an authentic or computer-generated NCII and outlines penalties for when the images of “intimate visual depiction” as defined in 15 USC 6851(5)(A), of an adult or minor and imposes new obligations on social media and online platforms to respond to requests to promptly remove unlawful NCII. Synthetic or computer-generated NCII, includes the term “digital forgery” meaning “any intimate visual depictions 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.” An identifiable individual includes someone “(i) who appears in whole or in part in an intimate visual depiction; and (ii) whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with such intimate visual depiction.”

Criminal Liability for “Knowingly” Publishing NCII

1. **Involving Adults**. The Act prohibits the use of an interactive computer service to knowingly publish an intimate visual depiction of an adult identifiable individual, who is not a minor, if (i) 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 reasonably expectation of privacy; (ii) what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting; (iii) what is depicted is not a matter of public concern; and (iv) publication of the intimate visual depiction is intended to cause harm or causes harm, including psychological, financial or reputational harm, to the identifiable individual. For synthetic or computer-generated digital forgeries, the test is similar, except to establish criminal liability, the depiction would have to be published without consent of the identified individual.
2. **Involving Minors**. Under the Act, NCII involving minors, defined as anyone under the age of 18 years, sets forth stricter prohibitions making it unlawful to publish NCII of an identifiable individual who is a minor with the intent to (i) abuse, humiliate, harass, or degrade the minor; or (ii) arouse or gratify the sexual desire of any person.
3. **Consent, Disclosure and Disclosure Exceptions**. The Act recognizes that the consent to create an image is not the same as consent to publication, stating that the fact that (i) an identifiable individual providing consent for the creation of an image; or (ii) the identifiable individual disclosure of the intimate visual depiction to another individual does not establish or constitute consent to publication. However, certain exceptions apply to allow for disclosure to law enforcement, professional obligation reporting requirements, or publication of an individual’s own images.

Civil Liability for Failure to Comply with Notice and Removal Requirements

The criminal provisions of the law went into effect immediately, the Act provides, "covered platforms" a year after the date the law went into effect, to develop a process for notice and removal of NCII identified from their platforms within 48 hours of receiving a valid request from an identifiable individual or someone authorized to act on the individual's behalf. A covered platform means "a website, online service, online application, or mobile application that (i) serves the public or (ii) for which it is the regular course of business of trade or business of the website, online service, online application, or mobile application to publish, curate, host or make available content of nonconsensual intimate visual depictions." Covered platforms do not include ISPs, email providers, online services that consist primarily of not user generated content, or services for which chat, comment or interactive functionality is directly related to the provision of not user generated content.

A covered platform must provide a clear, easy to understand and conspicuous policy which shall include valid removal request requirements, how to submit a removal request and the removal responsibilities of the platform. A valid removal request must be in writing, with a physical or electronic signature, and include (i) enough information to locate the depiction; (ii) a statement of the individuals' good faith belief that the depiction was not consensual; and (iii) the requester's contact information.

Within 48 hours of a valid removal request, the covered platform must remove the intimate visual depiction and make reasonable efforts to identify and remove any known identical copies of such depiction.

The Act gives covered platforms liability protections from claims from content posters based on the covered platforms good faith removal, disabling access to, or removal of, material claimed to be NCII, regardless of whether the intimate visual depiction is ultimately determined to be unlawful or not.

Covered Platform Next Steps

While the removal obligations will not take effect until May of 2026, covered platforms face significant obligations to confirm compliance. Knowledge of the Act allows companies to develop a business model to aid in immediate removal of NCIIs as it must occur with 48 hours. Therefore, companies that host user generated content, should prepare to take the following steps to determine if and how they would need to comply:

1. Determine if you or your company would be a covered platform.
2. Determine whether your company has enough resources, proper operating and escalation procedures, and training to implement the Act's requirements.
3. Establish a notice process and policy.
4. Review your data privacy, AI, cybersecurity, document retention and digital governance policies.
5. Consider engaging professional support to confirm that your company is prepared to comply with the Act's requirements.

Kristen Petrina is an associate in the Corporate and Commercial and Emerging Technologies groups of Babst Calland. She represents domestic and international clients on a broad range of general corporate and commercial law matters and advises businesses on data privacy and protection and security compliance.