



Cybersecurity and Information Security Newsletter

Issue 29 | June 30, 2025

Table of Contents

- [Federal anti-deepfake non-consensual intimate media bill, the "TAKE IT DOWN Act," signed into law](#)

Looking Ahead: On May 22, 2025, the House of Representatives passed House Resolution 1, "One Big Beautiful Act," which mainly focuses on the U.S. government's budgetary matters. As of June 30th, the Senate version of the bill includes a five-year moratorium for state and other non-federal government entities on regulating certain aspects of AI technologies. The next issue will address this latest U.S. government's preemption efforts on AI regulations.

Daniel Shin, W&M Adjunct Professor of Law and research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Federal anti-deepfake non-consensual intimate media bill, the “TAKE IT DOWN Act,” signed into law

On May 19, 2025, President Trump signed the “Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act” (TAKE IT DOWN Act),¹ enacting the first federal law that aims to address the spread of non-consensual intimate media created using generative AI techniques.

The law has two components. First, it makes the intentional disclosure of non-consensual intimate visual depictions a criminal violation that carries a fine and imprisonment. Second, it requires certain online platforms to create a process allowing individuals to submit a takedown request to the online platform to remove the non-consensual intimate visual imagery depicting the requesting person.

Deepfake and non-consensual intimate media history

“Deepfake” refers to synthetic but realistic media created using generative AI tools. Deepfake proliferation began when, on January 8, 2018, an anonymous user on the social media platform Reddit published “FakeApp,” the first deepfake video face-swapping tool that utilized various machine learning algorithms.² With the release of FakeApp and other face-swap deepfake creation tools, people with consumer-level gaming computers could create realistic face-swapped videos that replaced an individual’s face in a video with another with ease. The broader consequence of these tools was the proliferation of face-swapped pornography of women celebrities that were posted across social media networks.³

In response to public outcry, many social media platforms prohibited the posting of non-consensual intimate media on their websites.⁴ Meanwhile, deepfake creation tools were *de facto* permitted to be developed and shared on public software development platforms until, on August 22, 2024, GitHub, an online program developer platform, changed its terms of service enforcement and disabled the code repository for “DeepFaceLab,” one of the most popular face swap deepfake software in the deepfake

¹ White House, “President Trump and First Lady Melania sign the Take It Down Act into law in the Rose Garden”, <https://www.whitehouse.gov/videos/president-trump-and-first-lady-melania-sign-the-take-it-down-act-into-law-in-the-rose-garden/>.

² deepfakeapp, “FakeApp: A Desktop Tool for Creating Deepfakes”, https://www.reddit.com/r/deepfakes/comments/7ox5vn/fakeapp_a_desktop_tool_for_creating_deepfakes/ [archived URL: <https://archive.ph/OuIDc>].

³ Samantha Cole, “We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now”, <https://www.vice.com/en/article/reddit-fake-porn-app-daisy-ridley/>.

⁴ Pingupin, “Deepfakes banned, why?”, https://www.reddit.com/r/artificial/comments/7w0h74/deepfakes_banned_why/.

community. Other face swap deepfake tools have subsequently been disabled on GitHub as well.⁵

Despite the wide prohibition on uploading non-consensual intimate media on major social media platforms, websites dedicated to hosting and publishing deepfake videos provided alternate venues for deepfake creators to post their face swap video content for the web audience.

For instance, MrDeepFakes was one of the largest deepfake video-sharing websites that included its own forum for users to exchange information about deepfake video creation. The website even allowed deepfake creators to accept commissions to create specific deepfake videos of a particular (non-consenting) victim. After a few years of operation, on May 4, 2025, MrDeepFakes posted a “Shutdown Notice,” stating that a “critical service provider has terminated service permanently” and MrDeepFakes would permanently shut down.⁶

MrDeepFakes shutdown coincided with journalist investigations that uncovered the identity of one of the individuals running the website. On January 3, 2025, the German publication Der Spiegel published an extensive report on the deepfake community and MrDeepFakes, which included a partially redacted name of an individual living in Toronto, Canada, who was one of many allegedly running the deepfake video platform.⁷ On May 7, 2025, a Netherland-based investigative journalism website (with the collaboration of other news organizations) published an article on the same individual with his full name and other personal information fully revealed.⁸ As of publishing this newsletter article, MrDeepFakes is offline.

Face swaps and other forms of deepfake tools are still widely available. Furthermore, other deepfake pornography websites are still accessible and being actively used by deepfake creators and their audiences. However, the proactive efforts by academics, journalists, and organizations, in conjunction with indirect public coercion by those in government, are generating significant pressure against deepfake communities, likely constraining some of the proliferation of deepfake videos out on the open web and, more

⁵ FitContribution2946, “GitHub has removed access to roop-unleashed. The app is largely irrelevant nowadays but still a curious thing to do.”, https://www.reddit.com/r/StableDiffusion/comments/1i7n81a/github_has_removed_access_to_roopunleashed_the/.

⁶ MrDeepFakes.com, “Shutdown Notice”, <https://mrdeepfakes.com/shutdown.html> [archived webpage: <https://web.archive.org/web/20250504113218/https://mrdeepfakes.com/shutdown.html>].

⁷ Max Hoppenstedt, Roman Höfner, Marvin Milatz, Christo Buschek, and Markus Böhm, “The Growing Problem of Fake Porn Images”, <https://www.spiegel.de/international/zeitgeist/artificial-intelligence-and-deepfakes-the-growing-problem-of-fake-porn-images-a-82fd8d6c-f4e3-4237-9066-978cbcd496cf>.

⁸ Ross Higgins, Connor Plunkett, Beau Donnelly, George Katz, Kolina Koltai, and Galen Reich, “Unmasking MrDeepFakes: Canadian Pharmacist Linked to World’s Most Notorious Deepfake Porn Site”, <https://www.bellingcat.com/news/2025/05/07/canadian-pharmacist-linked-to-worlds-most-notorious-deepfake-porn-site/>.

likely, forcing the migration of deepfake creators and their audience deeper into the non-visible parts of the web, including the dark web.

Past Legislative Efforts and the TAKE IT DOWN Act

Since 2019, Congress has introduced various legislation that attempted to address the threat of deepfakes and their creation tools. For instance, the Consolidated Appropriations Act, 2021,⁹ which became law on December 27, 2020, included the “American Competitiveness Of a More Productive Emerging Tech Economy Act,” which required the Secretary of Commerce and the Federal Trade Commission to complete a study of the state of AI industry and its impact on the national economy.¹⁰ In the Act, Congress directed the Federal Trade Commission to conduct a study “on how [AI] may be used to address the online harms” such as “[m]anipulated content intended to mislead individuals, including deepfake videos and fake individual reviews.”¹¹

Although Congress did not pass any legislation that specifically criminalized deepfake media creation or its distribution prior to the TAKE IT DOWN Act, state governments passed legislation to address the deepfake threats. For example, on March 24, 2025, Virginia Governor Glenn Youngkin signed Senate Bill 1053, “Synthetic digital content; definition, penalty, report, effective clause.”¹² The bill expanded the state’s slander and libel laws to include synthetic digital content¹³ as “words” when an individual in effect engages in defamation, an act of slander or libel.¹⁴ Senate Bill 1053 effectively ensures that victims who were harmed by insulting deepfake media have the legal means to pursue the alleged slander or libel perpetrators who used deepfakes to commit tortious acts.

Other countries have taken a more aggressive posture on non-consensual intimate deepfake media. For instance, on October 16, 2024, the Republic of Korea amended its “Special Act on the Punishment of Sexual Crimes” to not only criminalize the creation of non-consensual intimate deepfake media but also the *possession, purchase, and storage* of such media.¹⁵

⁹ H.R.133 - Consolidated Appropriations Act, 2021, 134 STAT. 1182, <https://www.congress.gov/bill/116th-congress/house-bill/133>.

¹⁰ *Id.* at 3276.

¹¹ *Id.* at 3289.

¹² Legislative Information System, “SB1053: Synthetic digital content; definition, penalty, report, effective clause.”, <https://lis.virginia.gov/bill-details/20251/SB1053>.

¹³ Defined as “any digital content, including any audio, image, text, or video, that realistically but falsely depicts an individual’s appearance, speech, or conduct” that is produced using machine learning-based systems.

¹⁴ Virginia General Assembly, “SB1053: Synthetic digital content; definition, penalty, report, effective clause.”, <https://lis.blob.core.windows.net/files/1074288.PDF>.

¹⁵ 법제처 (Korea Ministry of Government Legislation), 성폭력범죄의 처벌 등에 관한 특례법 (Special Act on the Punishment of Sexual Crimes), <https://www.law.go.kr/%EB%B2%95%EB%A0%B9%EC%84%B1%ED%8F%AD%EB%A0%A5%EB%B2%94%EC%A3%84%EC%9D%98%EC%B2%98%EB%B2%8C%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%ED%8A%B9%EB%A1%80%EB%B2%95> (under 제 14 조의 2(허위영상물 등의 반포등)).

TAKE IT DOWN Act Provisions

As already noted, the TAKE IT DOWN Act has two major components: (1) the criminalization of intentional disclosures of non-consensual intimate media and (2) mandating the creation of a timely process for takedown requests for removing non-consensual intimate media on web platforms.

First, the TAKE IT DOWN Act prohibits the publishing of the intimate visual depiction of another who is an adult if:

- (1) the depiction was obtained or created under situations in which the person knew or reasonably should have known that the identifiable individual had a reasonable expectation of privacy;
- (2) what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting;
- (3) what is depicted is not a matter of public concern; and
- (4) publication of the intimate visual depiction is intended to cause harm or causes harm (including psychological, financial, or reputation harm) to the identifiable individual.

If the identifiable individual is a minor, then the publishing of the intimate visual depiction is unlawful if there was intent to:

- (1) abuse, humiliate, harass, or degrade the minor; or
- (2) arouse or gratify the sexual desire of any person.

The TAKE IT DOWN Act also prohibits the publishing of digital forgery of an identifiable individual, with the law having nearly identical elements to establish criminal liability as the publishing of non-consensual intimate media. Finally, the Act penalizes intentional threats of publishing intimate visual depictions or digital forgeries depicting another. Criminal penalties include fines and imprisonment.

The TAKE IT DOWN Act also mandates the establishment of a takedown procedure for victims (or the victims' representatives) of non-consensual intimate media whose likeness was used in published deepfake media on online platforms. Under the Act, deepfake victims can submit takedown requests that identify deepfake media depicting themselves and verify that the media were published without their consent. Once the takedown request procedures are implemented, online platforms must remove the intimate visual media and any known identical copies of such depictions within 48 hours of receiving a takedown request. Under the Act, online platforms have until May 19, 2026, to implement their takedown request procedures.

Online platforms that are mandated by the Act's takedown request requirements include any website, online service, online application, or mobile application that serves the

public and (1) that provides primarily a forum for user-generated content (e.g., messages, videos, images, games, and audio files) or (2) that in its regular course of operations publish, curate, host, or make available content of non-consensual intimate visual media. The Act also empowers the Federal Trade Commission to enforce online platforms' compliance with the takedown requests under the Federal Trade Commission Act's prohibition of unfair or deceptive acts or practices by commercial entities.

Analysis

The enactment of the TAKE IT DOWN Act is a monumental first step for the U.S. government to address the threat of non-consensual intimate media proliferating on the web. By criminalizing the publishing of non-consensual intimate media, the Act puts non-consensual intimate media creators on notice that criminal penalties will be imposed for violations. Also, the Act ensures the prompt removal of non-consensual intimate media content through its takedown request requirements for online service providers. Victims now have the means to quickly submit their takedown requests and be assured that any other copies of their depicted non-consensual intimate media will be removed from the online platform.

Despite the Act fulfilling the need to address the threat of non-consensual intimate media, there are a few areas in which the Act comes up short. First, by limiting the criminality of deepfakes to the definition of intimate visual depictions under 15 U.S.C. § 6851,¹⁶ threat actors can simply create and publish deepfakes that fall outside the scope of the defined term, which could then nevertheless humiliate the depicted victim.

Second, the Act's focus on whether the deepfake media creator knew or reasonably should have known that the depicted individual in the intimate visual media had a reasonable expectation of privacy forecloses enforcement on intimate visual depictions of deceased individuals. Although some in the legal literature argue that there are some levels of "postmortem privacy" under certain circumstances,¹⁷ deceased individuals traditionally do not have privacy rights.¹⁸ As a result, a deceased individual whose likeness is depicted in a non-consensual intimate media may likely not have the required expectation of privacy to meet one of the key elements of the TAKE IT DOWN Act's criminal liability.

Third, although the Act empowers the Federal Trade Commission to enforce takedown procedures of online platforms, the failure to provide any new resources or specific responsibilities to the criminal enforcement of the spread of non-consensual intimate imagery may lead to a protracted government response in prosecuting appropriately

¹⁶ U.S. House of Representatives, 15 U.S.C. § 6851, [https://uscode.house.gov/view.xhtml?req=\(title:15%20section:6851%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:15%20section:6851%20edition:prelim)).

¹⁷ Anita L. Allen & Jennifer E. Rothman, "Postmortem Privacy", <https://michiganlawreview.org/journal/postmortem-privacy/>.

¹⁸ William L. Prosser, "Privacy", <https://lawcat.berkeley.edu/record/1109651/files/fulltext.pdf?ln=en> (page 408).

suspected deepfake creators. Due to the substantial spread of non-consensual intimate imagery across multiple online platforms, substantial investment in federal resources and assignment of responsibilities in law enforcement is required to prevent unlawful deepfake creations and, subsequently, decrease the number of deepfake victims.

Finally, the biggest missed opportunity for the TAKE IT DOWN Act is its lack of requirement for online platforms to disclose (or retain) information about the individual who initially posted the non-consensual intimate visual media to victims. While the Act's takedown provision disrupts the spread of deepfake media, depicted victims do not have an automatic statutory right to compel online platforms to provide information about the individual who published the deepfakes, which can be used to pursue civil litigation. Although law enforcement can compel information about users who published non-consensual intimate visual media with a court-authorized search warrant, the TAKE IT DOWN Act's lack of user data retention requirements may allow deepfake creators to scrub their tracks before law enforcement can pursue the digital trail.
