DOI:10.1145/3747203

James Grimmelmann

Law and Technology
Deconstructing the Take It Down Act

How the recently enacted Take It Down Act could affect online platforms.

On May 19, 2025, President Trump signed into law the Take It Down Act against deepfake pornography. It is the first major federal law on artificial intelligence (AI) in the U.S., and offers significant protection for victims of online abuse. Unfortunately, it could also be abused to take down harmless content and threaten platforms with political retribution.

In this column, I will review the history leading up to the Take It Down Act, discuss its provisions, and consider some of the ways it could be used and abused. This is the fifth in a series of *Communications* Law and Technology columns on the rapidly changing state of U.S. online speech law.

Background

The Take It Down Act targets the kind of material usually called "revenge porn": nude images of people, typically but not necessarily sexual, posted without their consent. The phrase is a little misleading, because revenge is just one of many motivations driving it. A more lawerly term, precise but bloodless, is "nonconsensual intimate imagery," or NCII.

Whatever it is called, the stories of its victims are heartbreaking. Jealous exes post nude selfie images sent to them by their ex-partners. Stalkers photoshop their object of obsession's face onto sex workers' naked bodies. Hackers trick teens into sharing naked videos, and then use the videos as blackmail. AI-powered apps let anyone make and share pictures undressed of celebrities—or their classmates.

As NCII became increasingly widespread in the 2000s, advocates for its victims found that the legal system was ill-prepared to deal with it. While NCII can overlap with obscenity, child pornography, hacking, harassment, extortion, and civil privacy laws, it has its own distinctive harms that other laws do not always capture. Many victims struggled to convince police, prosecutors, and judges to take their abuse seriously.

The new crimes in the Act are significant, but not groundbreaking.

The first significant attempts to fight back against NCII came in the early 2010s and picked up steam as the decade went on. Law professors including Mary Anne Franks and Danielle Citron worked with the Cyber Civil Rights Initiative and other advocacy groups to help state legislatures pass laws against NCII.

Even so, it has been slow going. For one thing, these laws were state laws, not federal. Victims, police, and prosecutors often faced jurisdictional obstacles in finding and taking action against perpetrators of Internet-facilitated abuse. For another, the federal law known as Section 230 shielded online platforms from responsibility for user-posted content, so some of them turned a blind eye to NCII.

More recently, rapid advances in generative AI have led to new deepfake tools capable of making photorealistic

President Donald Trump signed the Take It Down Act during a White House Rose Garden presentation in May 2025.

images of almost anything or anyone. Sadly but unsurprisingly, some of its most eager adopters have built tools to generate vast quantities of NCII of people they despise, lust after, or both. Privacy-based laws against distributing *actual* intimate images of people do not always cleanly apply to distributing *synthetic* images of them.

The Take It Down Act—short for the "Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act"—was intended to close these various gaps. Similar bills had been introduced previously in Congress, but First Lady Melania Trump made it a high priority when her husband was re-elected in 2024. It passed Congress by overwhelming margins in April of 2025 and was signed into law in May.

New Federal Crimes

The heart of the Take It Down Act is Section 2, which creates new federal crimes for publishing online NCII of an identifiable person without their consent. Significantly, it covers both actual photos (an "intimate visual depiction") and deepfakes (a "digital forgery"). Penalties include fines and up to three years in prison. An additional provision deals with the risk of blackmail by making it a crime to threaten to publish NCII of a person, even if the threat is never actually carried out.

The Act also includes a long list of exceptions. Most obviously, law enforcement and intelligence activities are exempted. Even though police officers have sometimes been among the worst offenders in image-based abuse—precisely because of their authority and access to evidence—such an exception is necessary to enable investigations and prosecutions. Similarly, disclosures in legal proceedings and reports of unwanted conduct are allowed, so that victims and their advocates can come forward safely.

There is also an exception for people who publish NCII of themselves. On one level, this is understandable, and consistent with the Act's goal of empowering people to make their own decisions about intimate images of themselves. But, as Professor Franks has observed, this exception also creates a potential loophole that would allow people to distribute images that include themselves along with others who do not consent. Some perpetrators of image-based abuse can be shamed into stopping if they lose their anonymity, but some others are truly shameless.

The new crimes in the Act are significant, but not groundbreaking. Bringing federal investigators and prosecutors into the picture will help victims, but most of what the Act covers was already illegal at the state level. The most significant feature of this part of the Act is its clear signal that deepfake NCII is just as serious a problem as photographic NCII. AI-generated problems need legal responses.

Notice and Takedown

The more dramatic provision of the Take It Down Act is Section 3, which creates a new notice and takedown regime for NCII. Platforms must allow people to submit notices that user-uploaded content is NCII of them. If so, the platform must remove the material, and prevent it from being uploaded again in the future. (Oddly, the takedown system as written only applies to

PHOTO BY DT PHOTS1/SHUTTERSTOCK.COM

photographs and not to deepfakes; as far as anyone has been able to tell, this is an oversight.)

This takedown system is loosely based on the copyright rules of Section 512, enacted as part of the Digital Millennium Copyright Act. Those rules give online platforms immunity from copyright liability for user-posted content, but only if they respond "expeditiously" to take down infringing material when it is pointed out to them in a formal notice by the copyright owner.

This development is not entirely surprising. Before the Take It Down Act, some victims of NCII sent Section 512 copyright notices to platforms to remove those images. Sometimes the victims were the copyright owners, because copyright law considered them the "authors" of photos they took of themselves. But in other cases, the copyright claims were just a way to get platform lawyers' attention.

At first glance, a notice and takedown system for NCII makes sense. The copyright takedown system works when platforms can sift valid copyright claims from baseless ones. For example, it is straightforward for YouTube to confirm that an uploaded video really is a copy of *The Wild Robot*.

Similarly, it is straightforward to tell whether material is intimate imagery or not. Indeed, major platforms already unfortunately have to employ people and deploy systems to tell whether images are child pornography. The new takedown system should not be easy to abuse to send notices against arbitrary non-NCII content—at least if platforms diligently vet takedown notices.

Cause for Concern

Many of the Take It Down Act's differences from Section 512, however, give more cause for concern. Some copyright owners, and some fraudsters, send Section 512 takedown notices against completely innocent material. For example, this is a common technique used by shady reputation-management companies to help their clients get rid of unflattering news stories.

This is why Section 512 has a counter-notice procedure. A user who receives a takedown notice can send a counter-notice explaining that it is not infringing. If they do, the platform is allowed to put the material back up. The Take It Down Act has no such safety valve, which means that platforms may take down completely innocuous content.

The copyright takedown system works when platforms can sift valid copyright claims from baseless ones.

Amplifying this concern, the Take It Down takedown system lacks some of Section 512's safeguards against truly fraudulent notices. There is no liability for sending knowingly false notices, and no requirement that anything in the notice be made under penalty of perjury, so senders face little to no risk even for massively overclaiming. Censorious prudes might falsely claim to represent victims of NCII to take down fully consensual posts by sex workers, sexual and medical educators, and others. And even harassers—the very people the Act is meant to target—could in some circumstances use its takedown notices to suppress their victims' self-expression.

President Trump himself has shown how real this danger is. In his speech urging Congress to pass the Act, he said, "I'm going to use that bill for myself too if you don't mind, because nobody gets treated worse than I do online, nobody." A man who sues newspapers and television networks over factually true stories he disagrees with will not be shy about using Take It Down notices to censor criticism of himself.

Problematic Public Enforcement

It is also notable, and worrying, that the Take It Down Act's takedown provisions rely on public rather than private enforcement. It does not let victims sue platforms for ignoring valid takedown requests. (They can sue the uploaders, but often the uploaders will be anonymous or hard to sue; this is why some advocates were pushing for a takedown system.) Instead, the Federal Trade Commission can treat a platform's failure to implement a reasonable takedown system as an unfair or deceptive practice, and can impose fines or order changes.

At other times or in other countries, government enforcement might be a reasonable way to motivate platforms without imposing on them the threat of immense damages in private lawsuits. But in 2025 in the U.S., this kind of broad but vague enforcement power is itself a serious danger to the health of the Internet. The Trump administration has not been shy about pressuring Internet platforms to promote content praising him and to downrank criticism. It is easy to imagine the FTC weaponizing its newfound Take It Down Act authority as a tool of censorship and extortion.

In particular, it is easy to envision the FTC taking an extremely expansive position on the definition of an "intimate visual depiction" while also being exceptionally stringent about what counts as a "reasonabl[e]" takedown policy. Platforms might well be forced to remove LGBTQ+ content, sexual education materials, and much else on the basis of dubious takedown requests from censorious vigilantes. The administration could also use the threat of massive Take It Down Act liability to coerce the platforms in other ways, suppressing political speech the administration dislikes, or extracting payoffs to make FTC investigations go away.

All in all, then, the Take It Down Act is two steps forward and one step back—by the side of a gaping chasm. Its much-needed federal response to NCII could come with a high price tag for Internet freedom. The Act itself seems only to be about pornographic images, but it is broad enough that it could also be used as a tool of censorship and government control. Fortunately, most Internet users do not post NCII. Unfortunately, the Take It Down Act could restrict what all of us can post. C

James Grimmelmann (james.grimmelmann@cornell.edu) is the Tessler Family Professor of Digital and Information Law at Cornell Tech and in the Law School at Cornell University, New York, NY, USA.