

The Take It Down Act: A Censorship Weapon Disguised as Protection

A shoot-first-ask-questions-later censorship mechanism with no recourse.

By Christina Maas

6 min. read · [View original](#)

President Trump has thrown his support behind the [Take It Down Act](#), a bill designed to combat the spread of non-consensual intimate imagery (NCII), including AI-generated deepfakes. The legislation has gained momentum, particularly with First Lady Melania Trump [backing the effort](#), and Trump himself endorsing it during his March 4 address to Congress.

We obtained a copy of the bill for you [here](#).

“The Senate just passed the Take It Down Act.... Once it passes the House, I look forward to signing that bill into law. And 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.”

While this comment was likely tongue-in-cheek, it highlights an important question: how will this law be enforced, and who will benefit the most from it?

A Necessary Law with Potential Pitfalls

The rise of AI-generated explicit content and the increasing problem of revenge porn are serious concerns. Victims of NCII have long struggled to get harmful content removed, often facing bureaucratic roadblocks while the damage continues to spread. The Take It Down Act aims to give individuals more power to protect themselves online.

However, as with many internet regulations, the challenge is in the details. Laws designed to curb harmful content often run the risk of being too broad, potentially leading to overreach. Critics warn that, without clear

safeguards, the legislation could be used beyond its intended purpose.

The Free Speech Debate

The bill's language could allow well-funded individuals and public figures to demand takedowns of content they claim is "non-consensual," even when those claims are debatable. While protecting privacy is crucial, there is a fine line between removing harmful material and suppressing legitimate speech.

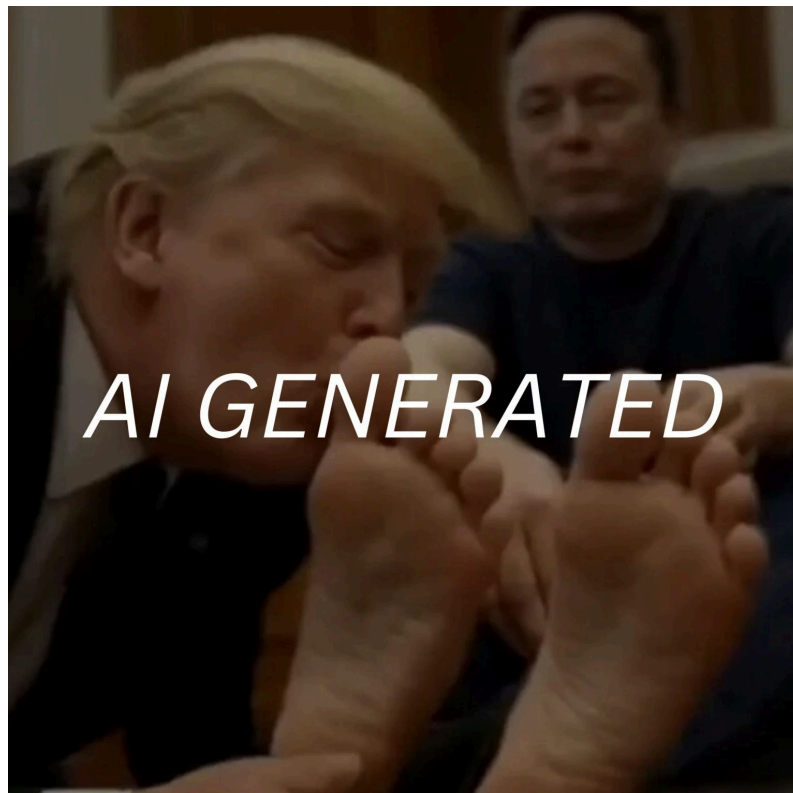
Supporters argue that tech companies have been slow to act against NCII, and stronger measures are necessary.

Meanwhile, civil liberties advocates worry that enforcement mechanisms could be misused, leading to potential censorship of investigative journalism, political commentary, or satirical content.

In its current form, the Take It Down Act transforms the internet into a legal minefield where speech, satire, and political criticism can be erased at the whim of the powerful. By failing to require proof before content is removed, the bill creates a system where accusations alone are enough to justify censorship. That means politicians,

celebrities, and corporations will have a new, government-backed method to scrub the internet of anything they find inconvenient.

Recent incidents highlight just how dangerously subjective the bill's definitions are. An AI-generated video of Trump and Elon Musk, depicting the president kissing Musk's feet, recently went viral.



Under the language of the Take It Down Act, such a video could arguably fall under the category of NCII, even though it contains no nudity or explicit content. The bill defines violations as involving an “identifiable individual” engaged in

“sexually explicit conduct,” a vague standard that leaves room for expansive interpretation.

Similarly, during the 2024 election, an image of then-Vice President Kamala Harris and her running mate Tim Walz was circulated online. The image showed the two candidates as characters from the movie Dumb and Dumber, with the two characters squeezing each other’s nipples. Meta [censored the image](#) suggesting that it was sexual.



The bill’s vague wording — especially its reference to “sexually explicit conduct” without a clear definition — only adds to the problem. If a satirical meme can be flagged as NCII simply because it portrays an “identifiable individual” in a suggestive manner, then what’s stopping the next administration from taking this to its logical extreme?

Think back to The Babylon Bee, the satirical website that was repeatedly penalized by social media platforms for making jokes about political figures. Or consider the countless deepfake memes that flood the internet during every election cycle — often ridiculous, often crude, but undeniably a form of political speech. Under this bill, such content could be wiped from existence with no oversight, no appeals process, and no accountability.

And let's not pretend that social media companies will put up much resistance. Given the choice between removing content immediately or risking federal action, they'll do what they always do— censor first, ask questions never.

Selective Enforcement and Political Power Plays

Even more concerning is how the Take It Down Act could be selectively enforced. Since platforms are required to comply with takedown requests in just 48 hours, whoever controls the mechanisms of enforcement — whether it's the Federal Trade Commission (FTC) or another regulatory body — will have an outsized

influence on what content stays online and what disappears.

History has shown us that these kinds of regulations are rarely applied evenly. During the COVID-19 pandemic, for instance, social media platforms took aggressive action against content that challenged the prevailing government narrative, while allowing misinformation from “approved” sources to spread unchecked. Imagine a future where a government agency wields similar discretion over what qualifies as NCII.

Once a censorship mechanism like this is in place, it won't just be politicians using it — it will be corporations, billionaires, and anyone with the legal firepower to threaten compliance. Journalists investigating corporate misconduct could find their work erased because a company claims an accompanying image violates NCII protections. Whistleblowers could have their evidence suppressed under the same pretext.

The biggest beneficiaries of the Take It Down Act won't be victims of online exploitation. They'll be the people who

already have the resources to control their public image.

At first glance, the Take It Down Act presents itself as a well-intentioned attempt to curb the spread of non-consensual intimate imagery (NCII). But beneath the surface, it operates more like a Trojan horse — promising protection while quietly handing the government and tech giants unprecedented control over online speech.

By placing enforcement under the Federal Trade Commission (FTC), the bill ensures that content moderation decisions will be subject to the whims of Washington's political landscape. Given the FTC's history of partisan regulatory actions, it's easy to predict how this could play out. Platforms that comply with government-preferred narratives will likely receive a lighter touch, while those that resist—or fail to police content to the administration's satisfaction—could find themselves in regulatory crosshairs.

It's an enforcement model ripe for abuse. Political figures with the right connections could see unflattering or

damaging content disappear almost overnight, while critics, independent journalists, and whistleblowers struggle against a system designed to suppress dissent.

The DMCA's Twin

This system bears a striking resemblance to the Digital Millennium Copyright Act (DMCA), which has long been [exploited for censorship](#). The DMCA's takedown process, originally intended to protect copyright holders, has been widely abused by corporations and individuals seeking to suppress critical or unfavorable content.

Platforms have to remove content when a complaint is made, and the complainant doesn't even have to offer proof that copyright has been violated. It also doesn't take into consideration fair use. The content has to be removed quickly and thus a censorship mechanism is easily created.

Automated Censorship and the End of Encrypted Privacy

One of the most overlooked yet deeply troubling aspects of the bill is its likely impact on encrypted messaging services.

Because the Take It Down Act makes platforms responsible for preventing the dissemination of NCII, companies may feel pressure to weaken encryption or introduce scanning mechanisms to comply with the law.

This would be a major step backward for digital privacy. End-to-end encryption is a cornerstone of secure communication, protecting everything from journalists' sources to everyday citizens' private conversations. If platforms are forced to monitor content proactively, it's only a matter of time before those surveillance capabilities are repurposed for other forms of content moderation, whether it be misinformation policing, political censorship, or government oversight of private communications.

A Pattern of Overreach

The Take It Down Act is part of a broader trend: lawmakers using real societal issues to justify sweeping new restrictions on speech and privacy. We've seen this before with proposals like the [Kids Online Safety Act \(KOSA\)](#), which was pitched as a way to protect children but ultimately raised concerns about online

copyright and parental control over content.

In each case, the pattern is the same: introduce legislation under the banner of safety, write it in vague and expansive terms, and leave enforcement in the hands of bureaucrats who can interpret it however they see fit. The result is a system where the rules can shift depending on who holds power—turning internet regulation into just another political weapon.

A Smarter Path Forward

If Congress truly wants to address NCII, there are far more effective ways to do so without trampling free expression and digital privacy. Here's what a responsible approach should include:

- Clear and narrow definitions of NCII prevent overreach and ensure satire, journalism, and fair-use content are protected.
- A burden of proof on those requesting takedowns, requiring them to demonstrate actual harm before content is removed.
- Stronger penalties for fraudulent claims deter abuse and prevent the system from being weaponized for censorship.

- Protections for encrypted communications, ensuring that platforms are not forced to weaken security measures in an attempt to comply.

The Take It Down Act, as it stands, does none of these things. Instead, it builds a broad, vague, and easily exploitable system that will almost certainly be used for purposes far beyond its stated goal.