## Taylor Swift and No Al Fraud Act: How Congress plans to fight back against Al deepfakes

abcnews.go.com/US/taylor-swift-ai-fraud-act-congress-plans-fight/story

Last week, the Internet was flooded with explicit, fabricated images of Swift.

ByLeah Sarnoff January 30, 2024, 11:36 AM

Taylor Swift's likeness was used for nonconsensual, seemingly AI-generated, deepfake pornography, which spread across the Internet like wildfire last week.

The mass circulation of the photos commanded headlines and re-confronted lawmakers with a question: Should U.S. citizens be federally protected against AI abuse?

The potential obscene ramifications of the Artificial Intelligence technology boom have long been feared by cyber civil rights organizations, such as CCRI, and are now seemingly unavoidable by the public and lawmakers alike.

Many social media users saw the explicit, fabricated images of Swift last week, which was met with decries from Swift's massive fanbase, "alarm" from the White House and outspoken fear of AI abuse from lawmakers such as Rep. Joe Morelle, D-NY, who is renewing efforts to make nonconsensual sharing of digitally-altered explicit images a federal crime, with jail time and fines.

One post on X that shared screenshots of the fabricated images of Swift was reportedly viewed over 47 million times before the account was suspended on Thursday, according to a New York Times report. X continued to suspend several accounts sharing the explicit images and made a "temporary action" to block all searches for Swift on the platform until Tuesday.

Elon Musk's social media platform re-enabled searches for Swift's name on Tuesday.

"Search has been re-enabled and we will continue to be vigilant for any attempt to spread this content and will remove it if we find it," Joe Benarroch, head of business operations at X, said in a statement, according to Associated Press.



Taylor Swift performs onstage during "Taylor Swift | The Eras Tour" at SoFi Stadium on August 09, 202... Kevin Winter/tas23 via Getty Images

Before being re-enabled, If a user searched for Swift on the site, a message appeared that reads: "Something went wrong. Try reloading," according to X.

Despite X's attempt to stop the rapid spread of these images on its platform, the photos have been shared on other social media sites and online spaces regardless of efforts to remove and block them.

"We are alarmed by the reports of the ... circulation of images that you just laid out -- of false images to be more exact, and it is alarming," White House Press Secretary Karine Jean-Pierre told ABC News on Friday.

A bipartisan group of U.S. House lawmakers -- led by Rep. María Elvira Salazar, R-Fla., alongside Reps. Madeleine Dean, D-Pa., Nathaniel Moran, R-Texas, Joe Morelle, D-N.Y., and Rob Wittman, R-Va., -introduced the No Artificial Intelligence Fake Replicas And Unauthorized Duplications (No AI FRAUD) Act on Jan. 10.

The lawmakers said they hope to create a federal, baseline protection against AI abuse and uphold Americans' First Amendment rights online.

## MORE: Fake explicit Taylor Swift images: White House is 'alarmed'

The bill aims to "establish a federal framework to protect Americans' individual right to their likeness and voice against AI-generated fakes and forgeries," according to Salazar's press release.

"What happened to Taylor Swift is a clear example of AI abuse. My bill, the No AI FRAUD Act, will punish bad actors using generative AI to hurt others — celebrity or not," Salazar said in a statement to ABC News. "Everyone should be entitled to their own image and voice and my bill seeks to protect that right."

In the past two years, AI technology has advanced, spread and become simplified from highly technical coding to user-friendly apps and websites, such as ChatGBT, that have fueled an entire online industry.

## MORE: How AI could affect jobs

Amid the AI boom, private companies are sprinting to create the most accessible tools for online users to create fabricated images, video, text and audio recordings of anything and everything they'd like. When a creator makes an AI-generated impersonation of a human, it's called a "deepfake."

Deepfake pornography, which Swift fell victim to, is often described as image-based sexual abuse.

The No AI FRAUD Act, if passed, would create a federal jurisdiction that will:

- Reaffirm that everyone's likeness and voice is protected and give individuals the right to control the use of their identifying characteristics.
- Empower individuals to enforce this right against those who facilitate, create and spread AI frauds without their permission.
- Balance the rights against First Amendment protections to safeguard speech and innovation.

"My thoughts are with Taylor Swift during this immensely distressing time. And my thoughts are with every other person who has been victimized by harmful AI deepfakes," Rep. Dean told ABC News in a statement. "If this deeply disturbing privacy violation could happen to Taylor Swift — TIME's 2023 person of the year — it is unimaginable to think how helpless other vulnerable women and children must also feel."

Rep. Dean continued, "at a time of rapidly evolving AI, it is critical that Congress creates protections against harmful AI. My and Rep. Maria Salazar's No AI FRAUD Act is intended to target the MOST harmful kinds of AI deepfakes by giving victims like Taylor Swift a chance to fight back in civil court."

## MORE: AI companies will need to start reporting their safety tests to the US government

Rep. Morelle said he hopes the abuse against Swift will be a driving force in getting the No AI FRAUD Act established.

"We're certainly hopeful the Taylor Swift news will help spark momentum and grow support for our bill, which as you know, would address her exact situation with both criminal and civil penalties," a spokesperson for Morelle told ABC News.

Since 2019, 17 states have enacted 29 bills focused on regulating the design, development and use of artificial intelligence, according to the Council of State Governments. However, not all have language that target the issue of pornographic deepfake, and the variety of language and destinctions allows for abuse to fall through the cracks, according to Salazar's press release.

"Laws at the state level to address these issues are inconsistent and, in some cases, not enough," the release notes.

Using Swift's possible case as an example, the singer has residences in Tennessee, New York, Rhode Island and California.



Taylor Swift performs onstage during "Taylor Swift | The Eras Tour" at SoFi Stadium, Aug. 9, 2023, in Inglewood, Calif.

Kevin Winter/TAS23/Getty Images for TAS Rights Management

Tennessee currently does not have a law that explicitly bans deepfake porn. However, Gov. Bill Lee proposed a bill this month -- the Ensuring Likeness Voice and Image Security (ELVIS) Act -- which aims to amend the state's Protection of Personal Rights law to include AI protection.

New York State does offer criminal and civil options for victims of deepfake abuse. In 2023, the state banned the distribution of pornographic images made using AI without the subject's consent. Violators in New York could face a \$1,000 fine and up to a year in jail.

"Since successfully expanding the right of publicity under New York State law I have been working to highlight the dangers of Artificial Intelligence and ensure we are taking steps to protect a person's likeness," Morelle said in the bill's press release. "Now it is apparent we must take immediate action to stop the abuse of AI technology by providing a federal law to empower individuals being victimized, and end AI FRAUD. I'm grateful to my colleagues for supporting this bipartisan effort and look forward to our work together stopping AI fakes and forgeries."

Rhode Island does not currently have deepfake or synthetic media laws.

California passed a law in 2020 to allow victims of nonconsensual, deepfake pornography to sue the creators and distributors for \$150,000 if the deepfake was "committed with malice."

Taylor Swift has not publicly commented on the AI deepfake images.

ABC News' Emmanuelle Saliba and Zohreen Shah contributed to this report.