# X ignores revenge porn takedown requests unless DMCA is used, study says

## Why did the study target X?

The University of Michigan research team worried that their experiment posting AI-generated NCII on X may cross ethical lines.

They chose to conduct the study on X because they deduced it was “a platform where there would be no volunteer moderators and little impact on paid moderators, if any” viewed their AI-generated nude images.

X’s transparency report seems to suggest that most reported non-consensual nudity is actioned by human moderators, but researchers reported that their flagged content was never actioned without a DMCA takedown.

Since AI image generators are trained on real photos, researchers also took steps to ensure that AI-generated NCII in the study did not re-traumatize victims or depict real people who might stumble on the images on X.

“Each image was tested against a facial-recognition software platform and several reverse-image lookup services to verify it did not resemble any existing individual,” the study said. “Only images confirmed by all platforms to have no resemblance to individuals were selected for the study.”

These more “ethical” images were posted on X using popular

hashtags like #porn, #hot, and #xxx, but their reach was limited to evade potential harm, researchers said.

“Our study may contribute to greater transparency in content moderation processes” related to NCII “and may prompt social media companies to invest additional efforts to combat deepfake” NCII, researchers said. “In the long run, we believe the benefits of this study far outweigh the risks.”

According to the researchers, X was given time to automatically detect and remove the content but failed to do so. It’s possible, the study suggested, that X’s decision to allow explicit content starting in June made it harder to detect NCII, as some experts had predicted.

To fix the problem, researchers suggested that both “greater platform accountability” and “legal mechanisms to ensure that accountability” are needed—as is much more research on other platforms’ mechanisms for removing NCII.

“A dedicated” NCII law “must clearly define victim-survivor rights and impose legal obligations on platforms to act swiftly in removing harmful content,” the study concluded.

https://arstechnica.com/tech-policy/2024/10/study-fastest-way-to-get-revenge-porn-off-x-is-a-dmca-takedown/

---

# Judge orders Google to distribute third-party app stores on Google Play

## Google plans appeal

Epic Games CEO Tim Sweeney wrote that the injunction “means all app developers, store makers, carriers, and manufacturers have 3 years to build a vibrant and competitive Android ecosystem with such critical mass that Google can’t stop it.”

Google issued a response saying it will appeal the underlying verdict and “will ask the courts to pause Epic’s requested changes, pending that appeal.”

The court-ordered “changes would put consumers’ privacy and security at risk, make it harder for developers to promote their apps, and reduce competition on devices,” Google VP of Regulatory Affairs Lee-Anne Mulholland wrote. “Ultimately, while these changes presumably satisfy Epic, they will cause a range of unintended consequences that will harm American consumers, developers and device makers.”

Mulholland also said the injunction will “undercut Android’s ability to compete with Apple’s iOS.”

“These Epic-requested changes stem from a decision that is completely contrary to another court’s rejection of similar claims Epic made against Apple—even though, unlike iOS, Android is an open platform that has always allowed for choice and flexibility like multiple app stores and sideloading,” she wrote.

## Judge dismisses Google arguments

Donato’s order allows Google to impose security restrictions on third-party apps, but he said that Google must show that any restrictions are necessary.

“As Google has suggested, there are potential security and technical risks involved in making third-party apps available, including rival app stores,” Donato wrote. “The Court is in no position to anticipate what those might be, or how to solve them. Consequently, Google will have room to engage in its normal security and safety processes. To the extent Google imposes requirements along these lines on rival app stores, it will… bear the burden when challenged of establishing that the requirements were strictly necessary to achieve safety and security for users and developers.”

https://arstechnica.com/tech-policy/2024/10/judge-orders-google-to-distribute-third-party-app-stores-on-google-play/

---

# Apple kicked Musi out of the App Store based on YouTube lie, lawsuit says

Musi is hoping a jury will agree that Apple breached its developer agreement and the covenant of good faith and fair dealing by removing Musi from the App Store. The music-streaming app has asked for a permanent injunction immediately reinstating Musi in the App Store and stopping Apple from responding to third-party complaints by removing apps without any evidence of infringement.

An injunction is urgently needed, Musi claimed, since the app only exists in Apple’s App Store, and Musi and its users face “irreparable damage” if the app is not restored. Additionally,

Musi is seeking damages to be determined at trial to make up for “lost profits and other consequential damages.”

“The Musi app did not and does not infringe any intellectual property rights held by Complainant, and a reasonable inquiry into the matter would have led Apple to conclude the same,” Musi’s complaint said.

On Reddit, Musi has continued to support users reporting issues with the app since its removal from the App Store. One longtime user lamented, “my heart is broken,” after buying a new iPhone and losing access to the app.

It’s unclear if YouTube intends to take Musi down forever with this tactic. In May, Wired noted that Musi isn’t the only music-streaming app taking advantage of publicly available content, predicting that if “Musi were to shut down, a bevy of replacements would likely sprout up.” Meanwhile, some users on Reddit reported that fake Musi apps keep popping up in its absence.

For Musi, getting back online is as much about retaining old users as it is about attracting new downloads. In its complaint, Musi said that “Apple’s decision has caused immediate and ongoing financial and reputational harm to Musi.” On Reddit, one Musi user asked what many fans are likely wondering: “Will Musi ever come back,” or is it time to “just move to a different app”?

Ars could not immediately reach Musi’s lawyers, Apple, or YouTube for comment.

https://arstechnica.com/tech-policy/2024/10/controversial-spotify-rival-musi-sues-apple-over-shady-youtube-takedown/

# Reports: China hacked Verizon and AT&T, may have accessed US wiretap systems

Chinese government hackers penetrated the networks of several large US-based Internet service providers and may have gained access to systems used for court-authorized wiretaps of communications networks, The Wall Street Journal reported Saturday. “People familiar with the matter” told the WSJ that hackers breached the networks of companies including Verizon, AT&T, and Lumen (also known as CenturyLink).

“A cyberattack tied to the Chinese government penetrated the networks of a swath of US broadband providers, potentially accessing information from systems the federal government uses for court-authorized network wiretapping requests,” the WSJ wrote. “For months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful US requests for communications data, according to people familiar with the matter.”

These “attackers also had access to other tranches of more generic Internet traffic,” according to the WSJ’s sources. The attack is being attributed to a Chinese hacking group called Salt Typhoon.

The Washington Post reported on the hacking campaign yesterday, describing it as “an audacious espionage operation likely aimed in part at discovering the Chinese targets of American surveillance.” The Post report attributed the information to US government officials and said an investigation by the FBI, other intelligence agencies, and the Department of Homeland Security “is in its early stages.”

The Post report said there are indications that China's Ministry of State Security is involved in the attacks.

## Verizon reportedly working with FBI

Verizon reportedly set up a war room at its facility in Ashburn, Virginia, where it is working with personnel from the FBI, Microsoft, and Google subsidiary Mandiant.

https://arstechnica.com/tech-policy/2024/10/reports-china-hacked-verizon-and-att-may-have-accessed-us-wiretap-systems/

---

# Elon Musk's X loses battle over federal request for Trump's DMs

"Going forward, the government will never have to prove it could avoid seriously jeopardizing its investigation by disclosing a warrant to only a trusted representative—a common alternative to nondisclosure orders," X argued.

In a brief supporting X, attorneys for the nonprofit digital rights group the Electronic Frontier Foundation (EFF) wrote that the court was "unduly dismissive of the arguments" X raised and "failed to apply exacting scrutiny, relieving the government of its burden to actually demonstrate, with evidence, that these alternatives would be ineffective."

Further, X argued that none of the government's arguments for

nondisclosure made sense. Not only was Smith's investigation announced publicly—allowing Trump ample time to delete his DMs already—but also "there was no risk of destruction of the requested records because Twitter had preserved them." On top of that, during the court battle, the government eventually admitted that one rationale for the nondisclosure order—that Trump posed a supposed "flight risk" if the search warrant was known—"was implausible because the former President already had announced his re-election run."

X unsuccessfully pushed SCOTUS to take on the Trump case as an "ideal" and rare opportunity to publicly decide when nondisclosure orders cross the line when seeking to seize potentially privileged information on social media.

In its petition for SCOTUS review, X pointed out that every social media or communications platform is bombarded with government data requests that only the platforms can challenge. That leaves it up to platforms to figure out when data requests are problematic, which they frequently are, as "the government often agrees to modify or vacate them in informal negotiations," X argued.

But when the government refuses to negotiate, as in the Trump case, platforms have to decide if litigation is worth it, risking sanctions if the court finds the platform in contempt, just as X was sanctioned $350,000 in the Trump case. If a less restrictive alternative was determined appropriate by the courts, such as appointing a trusted representative, platforms would never have had to guess when data requests threaten to expose their users' privileged information, X argued.

https://arstechnica.com/tech-policy/2024/10/elon-musks-x-loses-battle-over-federal-request-for-trumps-dms/

# SCOTUS denial ends saga of Shkreli's infamous 5,000% drug price scheme

The legal saga over Martin Shkreli's infamous 5,000 percent price hike of a life-saving anti-parasitic drug has ended with a flat denial from the highest court in the land.

On Monday, the Supreme Court rejected Shkreli's petition to appeal an order to return $64.6 million in profits from the pricing scheme of Daraprim, a decades-old drug used to treat toxoplasmosis. The condition is caused by a single-celled parasite that can be deadly for newborns and people with compromised immune systems, such as people who have HIV, cancer, or an organ transplant.

Federal prosecutors successfully argued in courts that Shkreli orchestrated an illegal anticompetitive scheme that allowed him to dramatically raise the price of Daraprim overnight. When Shkreli and his pharmaceutical company, Vyera (formerly Turing), bought the rights to the drug in 2015, the price of a single pill jumped to $750 after being priced between $13.50 and $17.50 earlier that year. And Shkreli quickly came to epitomize callous greed in the pharmaceutical industry.

In a lawsuit filed in 2021, the Federal Trade Commission and seven state attorneys general accused Shkreli of building a "web of anticompetitive restrictions to box out the competition." In January of 2022, US District Court Judge Denise Cote agreed, finding that Shkreli's conduct was "egregious, deliberate, repetitive, long-running, and ultimately dangerous."

https://arstechnica.com/tech-policy/2024/10/scotus-denial-ends-saga-of-shkrelis-infamous-5000-drug-price-scheme/

---

# FCC lets Starlink provide service to cell phones in areas hit by hurricane

The Federal Communications Commission gave Starlink and T-Mobile emergency authority to provide satellite-to-phone coverage in areas hit by Hurricane Helene.

“SpaceX and T-Mobile have been given emergency special temporary authority by the FCC to enable Starlink satellites with direct-to-cell capability to provide coverage for cell phones in the affected areas of Hurricane Helene,” SpaceX said yesterday. “The satellites have already been enabled and started broadcasting emergency alerts to cell phones on all networks in North Carolina. In addition, we may test basic texting (SMS) capabilities for most cell phones on the T-Mobile network in North Carolina.”

SpaceX warned of limits since the service isn’t ready for a commercial rollout. “SpaceX’s direct-to-cell constellation has not been fully deployed, so all services will be delivered on a best-effort basis,” the company said.

Starlink is being used to provide wireless emergency alerts to cell phones from all carriers in North Carolina, according to Ben Longmier, senior director of satellite engineering for

SpaceX. “We are also closely monitoring Hurricane Milton and standing by ready to take action in Florida,” he wrote.

## Temporary spectrum authority

The FCC said the approval “enabl[es] SpaceX to operate Supplemental Coverage from Space (SCS) in the 1910–1915 MHz and 1990–1995 MHz frequency bands leased from T-Mobile in areas affected by the Hurricane Helene.” An FCC spokesperson told Ars that the approval is for all areas affected by Hurricane Helene, although it’s only active in North Carolina so far.

The FCC also said that it is granting “special temporary authorities to licensees and issuing rule waivers to help communications providers maintain and restore service, support emergency operations, and assist public safety, including search and rescue efforts.” Separately, the FCC last week waived certain Lifeline program eligibility rules to help people in disaster areas apply for discounted phone and broadband service.

SpaceX began launching satellites with direct-to-cell capabilities in January 2024 and showed a demo of text messages sent between T-Mobile phones via one of Starlink’s low-Earth orbit satellites. T-Mobile has said the Starlink service for phones will help cover gaps in areas where it has no coverage “due to terrain limitations, land-use restrictions,” and other factors.

https://arstechnica.com/tech-policy/2024/10/fcc-lets-starlink-provide-service-to-cell-phones-in-areas-hit-by-hurricane/

# Smart TVs are like “a digital Trojan Horse” in people’s homes

Similarly, the report’s authors describe concerns that the CTV industry’s extensive data collection and tracking could potentially have a political impact. It asserts that political candidates could use such data to run “covert personalized campaigns” leveraging information on things like political orientations and “emotional states”:

> *With no transparency or oversight, these practices could unleash millions of personalized, manipulative and highly targeted political ads, spread disinformation, and further exacerbate the political polarization that threatens a healthy democratic culture in the US.*

## “Potential discriminatory impacts”

The CDD’s report claims that Black, Hispanic, and Asian-Americans in the US are being “singled out by marketers as highly lucrative targets,” due to fast adoption of new digital media services and brand loyalty. Black and Hispanic communities are key advertising targets for FAST channels, per the report. Chester told Ars:

> *There are major potential discriminatory impacts from CTV’s harvesting of data from communities of color.*

He pointed to “growing widespread racial and ethnic data” collection for ad targeting and marketing.

“We believe this is sensitive information that should not be applied to the data profiles used for targeting on CTV and across other platforms. … Its use in political advertising on CTV will enable widespread disinformation and voter suppression campaigns targeting these communities,” Chester said.

## Regulation

In a letter sent to the FTC, FCC, California attorney general, and CPPA , the CDD asked for an investigation into the US’ CTV industry, “including on antitrust, consumer protection, and privacy grounds.” The CDD emphasized the challenges that streamers—including those who pay for ad-free streaming—face in protecting their data from advertisers.

“Connected television has taken root and grown as an unregulated medium in the United States, along with the other platforms, devices, and applications that are part of the massive internet industry,” the report says.

The group asks for the FTC and FCC to investigate CTV practices and consider building on current legislation, like the 1988 Video Privacy Protection Act. They also request that antitrust regulators delve deeply into the business practices of CTV players like Amazon, Comcast, and Disney to help build “competition and diversity in the digital and connected TV marketplace.”

https://arstechnica.com/gadgets/2024/10/streaming-industry-has-unprecedented-surveillance-manipulation-capabilities/

---

# Neo-Nazis head to encrypted SimpleX Chat app, bail on Telegram

“SimpleX, at its core, is designed to be truly distributed with no central server. This allows for enormous scalability at low cost, and also makes it virtually impossible to snoop on the network graph,” Poberezkin wrote in a company blog post published in 2022.

SimpleX’s policies expressly prohibit “sending illegal communications” and outline how SimpleX will remove such content if it is discovered. Much of the content that these terrorist groups have shared on Telegram—and are already resharing on SimpleX—has been deemed illegal in the UK, Canada, and Europe.

Argentino wrote in his analysis that discussion about moving from Telegram to platforms with better security measures began in June, with discussion of SimpleX as an option taking place in July among a number of extremist groups. Though it wasn’t until September, and the Terrorgram arrests, that the decision was made to migrate to SimpleX, the groups are already establishing themselves on the new platform.

“The groups that have migrated are already populating the platform with legacy material such as Terrorgram manuals and are actively recruiting propagandists, hackers, and graphic designers, among other desired personnel,” the ISD researchers wrote.

However, there are some downsides to the additional security provided by SimpleX, such as the fact that it is not as easy

for these groups to network and therefore grow, and disseminating propaganda faces similar restrictions.

“While there is newfound enthusiasm over the migration, it remains unclear if the platform will become a central organizing hub,” ISD researchers wrote.

And Poberezkin believes that the current limitations of his technology will mean these groups will eventually abandon SimpleX.

“SimpleX is a communication network rather than a service or a platform where users can host their own servers, like in OpenWeb, so we were not aware that extremists have been using it,” says Poberezkin. “We never designed groups to be usable for more than 50 users and we’ve been really surprised to see them growing to the current sizes despite limited usability and performance. We do not think it is technically possible to create a social network of a meaningful size in the SimpleX network.”

*This story originally appeared on wired.com.*

https://arstechnica.com/tech-policy/2024/10/neo-nazis-head-to-encrypted-simplex-chat-app-bail-on-telegram/

---

# YouTube fixes glitch that wrongly removed accounts, deleted videos

As a message highlighted above the thread warned YouTube users that there were “longer than normal wait times” for support requests, YouTube continually asked for “patience” and turned off the comments.

“We are very sorry for this error on our part,” YouTube said.

Unable to leave comments, thousands of users mashed a button on the support thread, confirming that they had “the same question.” On Friday morning, 8,000 users had signaled despair, and as of this writing, the number had notched up to nearly 11,000.

YouTube has not confirmed how many users were removed, so that’s likely the best estimate we have for how many users were affected.

On Friday afternoon, YouTube did update the thread, confirming that “all channels incorrectly removed for Spam & Deceptive Practices have been fully reinstated!”

While YouTube claims that all channels are back online, not all the videos mistakenly removed were reinstated, YouTube said. Although most of the users impacted were reportedly non-creators, and therefore their livelihoods were likely not disrupted by the bug, at least one commenter complained, “my two most-viewed videos got deleted,” suggesting some account holders may highly value the videos still missing on their accounts.

“We’re working on reinstating the last few videos, thanks for bearing with us!” YouTube’s update said. “We know this was a frustrating experience, really appreciate your patience while we sort this out.”

It’s unclear if paid subscribers will be reimbursed for lost access to content.

YouTube did not respond to Ars’ request to comment.

https://arstechnica.com/tech-policy/2024/10/youtube-fixes-glitch-that-wrongly-removed-accounts-deleted-videos/