Google defends auto-deletion of chats after US alleged it destroyed evidence

Getty Images | picture alliance

reader comments

25 with

Share this story

Google defended its use of “history-off chats” for many internal communications, denying the US government’s allegation that it intentionally destroyed evidence needed in an antitrust case. The history-off setting causes messages to be automatically deleted within 24 hours.

The US government and 21 states last month asked a court to sanction Google for allegedly using the auto-delete function on chats to destroy evidence and accused Google of falsely telling the government that it suspended its auto-deletion practices on chats subject to a legal hold. Google opposed the motion for sanctions on Friday in a filing in US District Court for the District of Columbia.

Google said it uses a “tiered approach” for preserving chats. “When there is litigation, Google instructs employees on legal hold not to use messaging apps like Google Chat to discuss the subjects at issue in the litigation and, if they must, to switch their settings to ‘history on’ for chats regarding the subjects at issue in the litigation, so that any such messages are preserved,” the Google filing said.

US: Google deleted chats by default

Google's filing came in response to the US arguing that Google should have disabled auto-delete by default instead of "abdicat[ing] its burden to individual custodians to preserve potentially relevant chat."

"Google consciously failed to preserve relevant evidence. The daily destruction of relevant evidence was inevitable when Google set a company-wide default to delete history-off chat messages every 24 hours, and then elected to maintain that auto-delete setting for custodians subject to a litigation hold," US Justice Department of Justice antitrust lawyers told the court on February 23.

The US and states' lawsuit against Google was filed in October 2020 and alleges that Google illegally maintains monopolies in the markets for search and search advertising through anticompetitive and exclusionary practices. The US said Google "had a duty to preserve employee chat messages" starting in 2019 when it became clear that litigation was imminent.

Google: US demanded too much

Google said the government plaintiffs "contend that the Federal Rules specifically mandate that Google should have applied a forced history on setting for *all* custodians for *all* chats created while the custodian was on legal hold, regardless of the possible relevance of the message to the litigation."

Advertisement

But federal rules only require "reasonable steps to preserve" information, Google pointed out. "Google's vast preservation efforts here—and specifically its methodology with respect to history-off chats—were 'reasonable steps' under the Rule," Google argued.

Google said the US and state attorneys general “have not been denied access to material information needed to prosecute these cases and they have offered no evidence that Google intentionally destroyed such evidence.” Google also argued that the objections came too late, alleging that the government knew before litigation began “that there was a subset of chats not automatically retained.”

“Plaintiffs’ motions are barred at the outset because they were on notice of Google’s approach to chats for years, yet did not object until well after the close of discovery. Those tactics should not be countenanced,” Google told the court.

US: Google falsely claimed it suspended auto-delete

Google said its November 2019 disclosures in an ESI (Electronically Stored Information) questionnaire “show that the distinction between ‘on-the-record’ and other chats was apparent to anyone who wanted to pursue the matter from the outset of DOJ’s investigation. For instance, the ESI Questionnaire response specifies that chat ‘messages are generally retained for a period of 30 days if they have been marked on-the-record, and potentially longer if on-the-record messages are on legal hold.'”

Google also said, “it is no secret how Google’s Chat product operates” because it’s a publicly available product and the Google Chat website explains the history-off feature.

The Justice Department’s motion last month said things happened very differently. “Google systematically destroyed an entire category of written communications every 24 hours” for nearly four years, the government motion said, continuing:

> *All this time, Google falsely told the United States that Google had “put a legal hold in place” that “suspends auto-*

> *deletion.” Indeed, during the United States’ investigation and the discovery phase of this litigation, Google repeatedly misrepresented its document preservation policies, which conveyed the false impression that the company was preserving all custodial chats. Not only did Google unequivocally assert during the investigation that its legal hold suspended auto-deletion, but Google continually failed to disclose—both to the United States and to the Court—its 24-hour auto-deletion policy. Instead, at every turn, Google reaffirmed that it was preserving and searching all potentially relevant written communications.*

The history-off chats are also a subject of dispute in a separate lawsuit filed by Epic Games, which alleged that Google illegally monopolized the market for distribution of mobile apps and mobile app payment processing on Android. Epic filed a motion to sanction Google for alleged spoliation of evidence in October.

https://arstechnica.com/?p=1925623

AI-faked images of Donald Trump’s imagined arrest swirl on Twitter

Enlarge / AI-generated photo faking Donald Trump’s possible arrest, created by Eliot Higgins using Midjourney v5.

reader comments

180 with

Share this story

As the world waits to see if former President Donald Trump will actually be indicted today over hush-money payments to porn star Stormy Daniels, AI-generated images began circulating on Twitter imagining what that arrest would look like. Showing Trump resisting arrest and being dragged off by police, the realistic but very fake photos have already been viewed by millions.

“Making pictures of Trump getting arrested while waiting for Trump’s arrest,” tweeted Eliot Higgins, who is the founder and creative director of Bellingcat, an independent international collective of researchers, investigators, and citizen journalists.

In a tweet, Higgins confirmed that he used the impressively realistic AI engine Midjourney v5 to generate the fake images.

Ars couldn’t immediately reach Higgins for comment on the images, some of which have been viewed 2.2 million times on Twitter as of this writing.

Twitter guidelines say that users “may not deceptively share synthetic or manipulated media that are likely to cause harm” and suggest that, at the very least, the images may soon be labeled to “help people understand their authenticity and to provide additional context.” Ars reached out to Twitter for comment on the images, but—as CEO Elon Musk tweeted the company would do days ago—Twitter only responded with a poop emoji.

Twitter’s failure to label the somewhat convincing AI-generated images could potentially cause harm, as The Guardian

reported that there has been a significant increase in online threats since news of Trump's potential indictment started spreading. AP News reported that New York is already preparing for possible unrest if an arrest happens, and some users have remarked that Higgins' images were convincing enough to fool them.

Advertisement

> *Legit thought these were real.*
>
> *— Chris Jancelewicz (@CJancelewicz) March 20, 2023*

> *We should really be putting watermarks on these that disclose they are AI generated and not real.*
>
> *— Matt Karolian (@mkarolian) March 20, 2023*

At least one Twitter user suggested Higgins should have put a watermark on the image to eliminate any potential confusion. But whether Higgins had any duty to do so remains one of those still-unanswered questions swirling online as AI-generated content becomes increasingly popular—creating a potential future where Internet users may be unable to believe anything they see online.

Midjourney could not immediately be reached to confirm whether Higgins' images violate its terms of service, which includes community guidelines that ban "images or use text prompts that are inherently disrespectful, aggressive, or otherwise abusive."

"Violence or harassment of any kind will not be tolerated," the guidelines say.

Social media platforms are beginning to lay out ground rules for AI-generated content, and at least some have put the onus on users to label such content. TikTok is the latest platform to require that all realistic deepfakes be "clearly

disclosed," prompting users this week to start adding a "sticker or caption, such as 'synthetic,' 'fake,' 'not real,' or 'altered'" to prevent confusion.

Anyone who clicks through Higgins' thread of AI-generated images faking Trump's arrest would likely realize that the images are not real. Not only do they show Trump resisting arrest and even running from police, but there are also images showing Trump seemingly prepared to tackle a cop and court scenes showing Trump sobbing, which could seemingly happen only well after any arrest.

Additionally, Higgins did arguably clearly label the images as fake in his initial tweet on the thread that says he's "making pictures" and in subsequent tweets describing the images as "AI Trump world."

https://arstechnica.com/?p=1925576

Antisemitism on Twitter has more than doubled since Elon Musk took over

Getty Images | Thomas Trutschel

reader comments

208 with

Share this story

In the days after Elon Musk took over Twitter in October 2022, the social media platform saw a “surge in hateful conduct,” which its then safety chief put down to a “focused, short-term trolling campaign.” New research suggests that when it comes to antisemitism, it was anything but.

Rather, antisemitic tweets have more than doubled over the months since Musk took charge, according to research that I and colleagues at tech firm CASM Technology and the Institute for Strategic Dialogue think tank conducted. Between June and October 26, 2022, the day before Twitter’s acquisition by Musk, there was a weekly average of 6,204 tweets deemed “plausibly antisemitic”—that is, where at least one reasonable interpretation of the tweet falls within the International Holocaust Remembrance Alliance’s definition of the term as “a certain perception of Jews, which may be expressed as hatred towards Jews.”

But from October 27 until February 9, 2023, the average was 12,762—an increase of 105 percent. In all, a total of 325,739 tweets from 146,516 accounts were labeled as “plausibly antisemitic” over the course of our study, stretching from June 1, 2022 to February 9, 2023.

Enlarge / A relatively flat level of antisemitic tweets more than tripled around the time Elon Musk took control of Twitter on October 27, 2022.
Ars Technica

Finding antisemitism with AI

To identify plausibly antisemitic tweets, my co-authors and I combined 22 published hate speech-identifying algorithms into a single mechanism and used even more machine learning to see which combinations of decisions led to the correct result. We then passed through all tweets—over a million in total—that contained any one of 119 words, phrases, slurs, and epithets related to antisemitism.

Advertisement
No such process is perfect. We estimate our model to make a correct decision about 75 percent of the time. We also no doubt missed some antisemitic tweets not containing any of

those 119 key words, as well as those taken down before early December when we collected the data.

We then used an algorithm to draw out 10 different themes of antisemitism seen in the tweets. Some centered around the use of specific antisemitic derogatory epithets. Others alluded to conspiracy theories concerning hidden Jewish influence and control.

Antisemitic tweets directed at Jewish investor and philanthropist George Soros warranted its own category. He was mentioned more than any other person in our data, over 19,000 times, with tweets claiming he was a member of a hidden globalist, Jewish, or "Nazi" world order.

Another theme were tweets defending the rapper Ye, formerly Kanye West, who had made a number of antisemitic remarks after he had his account briefly reinstated by Musk.

Our research, which has not yet been peer-reviewed, also found around 4,000 of the antisemitic tweets were focused on the Russian invasion of Ukraine. These variously claimed that the conflict was caused by Jews, or that Jews secretly caused the US to support Ukraine. They also contained direct antisemitism directed against the Ukrainian president, Volodymyr Zelenskyy, who is Jewish.

https://arstechnica.com/?p=1925490

Fighting VPN criminalization should be Big Tech's top

priority, activists say

Aurich Lawson | Getty Images

reader comments

36 with

Share this story

“Women, life, freedom” became the protest chant of a revolution still raging in Iran months after a 22-year-old Kurdish woman, Mahsa Amini, died while in custody of morality police. Amini was arrested last September for “improperly” wearing a hijab and violating the Islamic Republic’s mandatory dress code laws. Since then, her name has become a viral hashtag invoked by millions of online activists protesting authoritarian regimes around the globe.

In response to Iran’s ongoing protests—mostly led by women and young people—Iranian authorities have increasingly restricted Internet access. First, they temporarily blocked popular app stores and indefinitely blocked social media apps like WhatsApp and Instagram. They then implemented sporadic mobile shutdowns wherever protests flared up. Perhaps most extreme, authorities responded to protests in southeast Iran in February by blocking the Internet outright, Al Arabiya reported. Digital and human rights experts say motivations include controlling information, keeping protesters offline, and forcing protesters to use state services where their online activities can be more easily tracked—and sometimes trigger arrests.

As getting online has become increasingly challenging for

everyone in Iran—not just protesters—millions have learned to rely on virtual private networks (VPNs) to hide Internet activity, circumvent blocks, and access accurate information beyond state propaganda. Simply put, VPNs work by masking a user's IP address so that governments have a much more difficult time monitoring activity or detecting a user's location. They do this by routing the user's data to the VPN provider's remote servers, making it much harder for an ISP (or a government) to correlate the Internet activity of the VPN provider's servers with the individual users actually engaging in that activity.

But as demand for VPNs has peaked, authorities have recently started moving more intently to block VPN access. That includes potentially taking drastic steps like criminalizing the sale of VPNs. Ars couldn't reach the Iranian parliament to confirm what, if any, new restrictions may be coming. But experts told Ars that it's likely censorship will intensify. Seeming to confirm the ongoing escalation, Ruhollah Momen-Nasab, a parliamentary special adviser who is overseeing an Internet restriction bill condemned by more than 50 human rights groups, has recently called for VPN sellers to be executed.

Advertisement

VPN providers have not buckled under this intense pressure, though. Using a pseudonym to protect his identity under heightened government scrutiny, Lucas is a spokesperson for Lantern, one of Iran's oldest and most popular free VPN tools, with close to 9 million monthly active users in the country. Lucas told Ars that Lantern's traffic has grown by 400 percent since Amini's death, and because of that, server costs have skyrocketed. To keep VPN access stable while auto-scaling services to meet rising user demand, Lantern started taking donations, maxing out credit cards, and collaborating with other organizations providing VPN services in the area to troubleshoot connection issues as they arise.

“We’re constantly getting attacked by the Iranian government,” Lucas told Ars. “So we’re in this constant state of looking at the data, listening to users, and trying to come up with completely new techniques to keep everyone online.”

Censorship evolves daily

As part of a small group of organizations defending Internet access in Iran, Lantern helps people like Milad, a 35-year-old Lantern user who requested that Ars not use his full name while discussing his secret VPN use. Circumventing Internet blocks daily, Milad mostly relies on VPNs to “figure out which news is not as reliable” and to direct friends and family to “threads they should follow” so they can read beyond state propaganda and monitor how authorities are responding to protests. For Milad, getting online requires more than just one tool. He needs a complete toolbox of VPNs, anonymity networks, and varied proxy solutions—a personal arsenal of circumvention tools that he has been building for the past decade to stay ahead of ever-changing censorship tactics.

“Censorship here evolves weekly, if not daily,” Milad told Ars. “I use a few tools on a daily basis.”

Iran is behind only Russia as the nation most affected by Internet shutdowns, according to a report from Top10VPN, an independent review site that monitors VPN use and Internet shutdowns. Last year, Internet shutdowns cost the Iran economy $773 million—money that businesses lost during 130 hours of Internet throttling, 2,179 hours of Internet blackouts, and 4,863 hours of social media shutdowns. Globally, the cost to economies in 2022 was nearly $24 billion, which is more than 300 percent higher than shutdown costs in 2021.

https://arstechnica.com/?p=1923060

US investigates TikTok owner ByteDance’s surveillance of journalists

Getty Images | Chesnot

reader comments

32 with

Share this story

New reports say the US Justice Department is investigating TikTok-owner ByteDance over recent revelations that employees tracked journalists in an attempt to find out who leaked company data to the press.

The Justice Department and US Attorney in the Eastern District of Virginia “subpoenaed information from ByteDance regarding efforts by its employees to access US journalists’ location information or other private user data using the TikTok app,” Forbes reported yesterday. “According to two sources, the FBI has been conducting interviews related to the surveillance.”

The investigation was also confirmed today in New York Times and Wall Street Journal articles citing anonymous sources. The investigation reportedly began in December. ByteDance is based in China, and TikTok is facing the possibility of being banned in the US if it doesn’t sever ties with its China-based owners.

“We have strongly condemned the actions of the individuals found to have been involved, and they are no longer employed at ByteDance,” the company told Forbes this week. “Our internal investigation is still ongoing, and we will cooperate with any official investigations when brought to us.”

Surveillance targeted US and UK journalists

ByteDance’s internal investigation, which was triggered by news reports detailing the surveillance, “found that employees tracked multiple journalists covering the company, improperly gaining access to their IP addresses and user data in an attempt to identify whether they had been in the same locales as ByteDance employees,” Forbes wrote in December, adding:

> *The investigation, internally known as Project Raven, began this summer after BuzzFeed News published a story revealing that China-based ByteDance employees had repeatedly accessed US user data, based on more than 80 hours of audio recordings of internal TikTok meetings. According to internal ByteDance documents reviewed by Forbes, Project Raven involved the company’s Chief Security and Privacy Office, was known to TikTok’s Head of Global Legal Compliance, and was approved by ByteDance employees in China. It tracked Emily Baker-White, Katharine Schwab and Richard Nieva, three Forbes journalists that formerly worked at BuzzFeed News.*

Advertisement

The surveillance campaign “was designed to unearth the source of leaks inside the company following a drumbeat of stories exposing the company’s ongoing links to China,” Forbes wrote. The report said that ByteDance chief internal auditor Chris Lepitak was fired, while the China-based executive Lepitak reported to, Song Ye, resigned.

A Financial Times reporter was also reportedly targeted by the company's surveillance. "Two members of staff in the US and two in China gained access to the IP addresses and other personal data of FT journalist Cristina Criddle, to work out if she was in the proximity of any ByteDance employees, the company said. However, the company failed to find any leaks," the FT wrote in December.

Criddle wrote articles "revealing that dozens of staff had left TikTok's London office and that some had worked 12-hour days or had been demoted after taking time off," the FT wrote.

TikTok has said it would restructure the Internal Audit and Risk Control department and that it removed all user data access and permissions for the department. We contacted ByteDance today and will update this article if the company provides any further comment.

https://arstechnica.com/?p=1925004

Starlink/T-Mobile plan for satellite-to-phone service to get boost from FCC

Enlarge / SpaceX CEO Elon Musk and T-Mobile CEO Mike Sievert at a joint event on August 25, 2022, in Boca Chica Beach, Texas.
Getty Images | Michael Gonzalez

reader comments

73 with

Share this story

The Federal Communications Commission says it wants to help satellite companies and mobile carriers partner up to close gaps in wireless networks. In a 4-0 vote, the FCC yesterday proposed “a new regulatory framework” designed to help satellite operators and wireless companies “leverage the growth in space-based services to connect smartphone users in remote, unserved, and underserved areas.”

In August 2022, Starlink operator SpaceX and T-Mobile announced a plan to deliver space-to-ground service to mobile phones in areas not covered by T-Mobile’s cellular network. SpaceX said this week that the companies plan to start testing the satellite-to-cell service sometime this year. Text messaging is expected to be the first supported service, with voice and Internet coverage to be added later.

The FCC said yesterday that “numerous such collaborations have launched recently, and the FCC seeks to establish clear and transparent processes to support supplemental coverage from space.”

The FCC vote approved a Notice of Proposed Rulemaking (NPRM) that seeks public comment on a plan to regulate these collaborations and provide more access to spectrum needed to deliver the hybrid services. The NPRM “proposes a framework through which satellite operators collaborating with terrestrial service providers would be able to obtain FCC authorization to operate space stations on certain currently licensed, flexible-use spectrum allocated to terrestrial services,” the FCC said.

The FCC also said it is “proposing to add a mobile-satellite

service allocation on some terrestrial flexible-use bands." Operators of low-Earth orbit satellites, like Starlink, could "apply to access terrestrial spectrum if certain prerequisites are met, including a lease from the terrestrial licensee within a specified geographic area," the FCC said.

Advertisement

Emergency calls and texts in remote areas

If approved, a satellite operator "could then serve a wireless provider's customers should they need connectivity in remote areas, for example in the middle of the Chihuahuan Desert, Lake Michigan, the 100-Mile Wilderness, or the Uinta Mountains," the FCC said.

The FCC said it wants public comment on how the new regulatory framework can "best support access to emergency response systems like 911 and wireless emergency alerts when a consumer is connected via supplemental coverage from space." The agency is also looking for input "on whether the framework can be extended to other bands, locations, and applications that might be supported by such collaborations."

FCC Chairwoman Jessica Rosenworcel said the satellite/mobile collaborations initially may not provide high-speed broadband to phones. "But to start, they could deliver low-bandwidth connectivity suitable for emergency calls and texts in remote settings where terrestrial networks do not reach," she said.

Rosenworcel said new regulations are needed because "there are challenges with access to airwaves, frequencies that are not all globally aligned, possibilities for interference that must be managed, and standards work that could help grow these capabilities. But what is clear is that with the growing interest in the possibilities of convergence of satellite and

terrestrial services, an ad-hoc, case-by-case approach to these new ventures is not enough.”

Starlink/T-Mobile is one of several ventures

A draft of the NPRM released a few weeks before yesterday’s vote pointed out several satellite-to-phone services that are in the works. SpaceX and T-Mobile are proposing to “use a block of T-Mobile’s mid-band Personal Communication Services (PCS) spectrum held over a nationwide footprint,” the FCC said. Last month, “SpaceX filed an application with the Commission detailing its proposed partnered service, including a request for authorization for SpaceX to use T-Mobile’s PCS G block spectrum for ‘direct-to-cellular’ operations.” The application includes several requests for waivers from the FCC’s existing rules.

Advertisement

Outside the US, “Lynk Global has partnered with a number of mobile network operators (MNOs) around the world to enable their customers to send texts using Lynk’s satellite network,” the FCC said. “Like the SpaceX/T-Mobile proposal, Lynk has emphasized the public safety importance of this type of service during emergencies and natural disasters, such as hurricanes, wildfires, flooding, or earthquakes, which often cause the destruction of or damage to terrestrial mobile network equipment and resulting service outages.”

Lynk also filed an application with the FCC and “has received Commission authority to test communications between satellites and mobile devices,” the draft NPRM said.

Texas-based company AST SpaceMobile “deployed its test BlueWalker 3 satellite in November 2022, indicating its plans to develop a global network to provide service directly from its satellites to smartphones,” the FCC said. AST filed

applications to provide service in the US and “has partnered with several MNOs for its planned service, including AT&T and Vodafone, and the partnerships are described as being capable of bringing service to remote and ‘off-grid’ locations,” the FCC said.

Though AST has applied for market access, “its current request is limited to frequencies for feeder links only, with no current request for direct-to-handset market access,” the FCC said.

Bloomberg reported that the “FCC changed draft language that proposed barring the use of frequencies eyed for calls-via-satellite by AT&T and Midland, Texas-based startup AST SpaceMobile, and now seeks comments on allowing their use, agency staff said in a news conference. Those airwaves are assigned to FirstNet, a wireless network for public safety officials operated by AT&T. In filings, both AT&T and AST SpaceMobile had asked the FCC to allow direct-to-satellite service on the FirstNet airwaves, which are being used to test the service.”

https://arstechnica.com/?p=1924911

Inside Elon Musk’s cost-cutting drive at Twitter

FT montage/Getty Images/Bloomberg

reader comments

186 with

Share this story

From a secretive “war room” at Twitter’s San Francisco headquarters last month, Elon Musk’s trusted lieutenants pored over a list of employees, showing how much they cost the social media company.

The billionaire owner’s “transition team,” headed by Steve Davis, who leads the Musk-owned Boring Company, then began to phone staffers. Some were asked to justify their role; others to recommend which colleagues to retain.

Those deliberations informed Musk’s latest layoffs at Twitter, as part of his efforts to bring the lossmaking company to financial health while also battling an advertiser exodus and unwieldy debt servicing bill.

The February cuts removed more than 200 staff but were still broader and deeper than many employees had anticipated, because they came after Musk had already laid off half of the company’s 7,500 workforce following his acquisition of Twitter in October. The move wiped out large swaths of its business development and product teams, leaving Twitter leaner—and more unstable.

Advertisement

This account of the billionaire’s ongoing efforts to wrestle Twitter’s finances under control with his inner circle is based on interviews with current and former Twitter staffers, people aware of Musk’s thinking, and his public statements on Twitter and to investors.

Musk, Twitter, and most members of the transition team did not respond to a request for comment.

Formed in November, the transition team has often refused to immediately pay many of Twitter’s vendors, landlords, and partners in the hope of keeping down costs, in some cases irking clients and leading to frosty stand-offs.

This push comes as Twitter is expected to roll out new equity compensation packages for employees in late March, said two people familiar with the situation. For tax purposes, Twitter is in the process of calculating a new valuation to price the common equity in the business, which determines the value of staff stock options, the people said. One of them said the valuation would probably be far lower than the $44 billion acquisition price.

At an investor conference hosted by Morgan Stanley last week, Musk said he had cut non-debt expenditures to $1.5 billion, from the $4.5 billion that he claimed it would have otherwise incurred in 2023, adding that Twitter could reach positive cash flow by the second quarter.

https://arstechnica.com/?p=1924892

Authors risk losing copyright if AI content is not disclosed, US guidance says

reader comments

84 with

Share this story

As generative AI technologies like GPT-4 and Midjourney have rapidly gotten more sophisticated and their creative use has exploded in popularity, the US Copyright Office has issued guidance today to clarify when AI-generated material can be copyrighted.

Guidance comes after the Copyright Office decided that an author could not copyright individual AI images used to illustrate a comic book, because each image was generated by Midjourney—not a human artist. In making its decision, the Copyright Office committed to upholding the longstanding legal definition that authors of creative works must be human to register works. Because of this, officials confirmed that AI technologies can never be considered authors.

This wasn't the only case influencing new guidance, but it was the most recent. Wrestling with the comic book's complex authorship questions helped prompt the Copyright Office to launch an agency-wide initiative to continue exploring a wider range of copyright issues arising as the AI models that are used to generate text, art, audio, and video continue evolving.

The guidance offers some specifics on what isn't copyright eligible when it comes to AI works generated solely by prompts—with no modifications made—which the Copyright Office likens to giving "instructions to a commissioned artist." These works lack human authorship and, therefore, won't be registered.

When "AI technology receives solely a prompt from a human and produces complex written, visual, or musical works in response, the 'traditional elements of authorship' are determined and executed by the technology—not the human user," the guidance explains. "Based on the Office's understanding of the generative AI technologies currently available, users do

not exercise ultimate creative control over how such systems interpret prompts and generate material."

However, as in the Midjourney case, an author who arranges generative AI into a specific sequence—like designing the layout for a comic book—can potentially copyright that sequence of images, if the arrangement is "sufficiently creative." Similar logic applies if an author or artist has modified AI-generated materials, and "the modifications meet the standard for copyright protection." Examples could be modifying an AI image in Adobe Photoshop, or altering AI-generated audio by using guitar pedals, the guidance says.

Advertisement
It's clear, though, that the Copyright Office is only in the earliest stages of navigating these complex cases, and guidance remains somewhat vague. Ultimately, officials considering whether AI-assisted works were conceived by humans or by machines will reach decisions on a case-by-case basis, guidance says.

"The answer will depend on the circumstances, particularly how the AI tool operates and how it was used to create the final work," the guidance says.

Any AI-generated content must be disclosed

Perhaps the most significant aspect of the guidance is an author's "duty to disclose the inclusion of AI-generated content in a work submitted for registration."

When registering works, authors must distinguish which content is human-authored and which content is AI-generated. If applicants aren't sure how to refer to the AI-generated content, the Copyright Office recommends providing a general statement that the work contains AI-generated content. That

will prompt the office to follow up to help each author fill in the blanks in an application.

For artists who have pending applications or have already registered works that contain AI-generated content, the Copyright Office suggests correcting the public record by submitting a supplementary registration. Any failure to accurately reflect the role of AI in copyrighted works could result in "losing the benefits of the registration," the office warned. That could leave works vulnerable to being copied, with little or no legal recourse for copyright infringement claims.

Failure to disclose AI-generated content is the only type of infringement discussed in the guidance. Critics like Alex J. Champandard, a co-founder of Creative.ai—a group of hackers and artists interested in generative AI—tweeted to say that current guidance puts authors in a precarious catch-22 situation.

"By disclosing the AI, you're opening yourself up to infringement, but by not disclosing AI, it's safer but in violation of [the US Copyright Office]!" Champandard's tweet suggested.

Ars couldn't reach Champandard to discuss other concerns his group has about the guidance.

https://arstechnica.com/?p=1924741

Lawsuit: Cop pulled over

driver for TikTok livestream—and shared driver's ID

reader comments

88 with

Share this story

A Dallas County Sheriff's Department deputy, Francisco Castillo, was briefly suspended after livestreaming a traffic stop, allegedly just to gain TikTok clout, in 2021. Now, the Texas motorist that he pulled over, Torry Osby, is suing, saying that the deputy exposed Osby to risks of identity theft and break-ins at his home by flashing Osby's driver's license and sharing his personal information to more than 100 followers tuned into Castillo's livestream.

Osby's lawyer, James P. Roberts, told Ars that it's unlikely that their client was the only victim of Castillo's alleged privacy-invading social media abuse. The complaint documents a seeming pattern of Castillo sharing videos while on duty that seemed to get more engagement than his other videos, making it appear likely to Osby's lawyers that Castillo was increasingly motivated to create videos of his police activity in hopes of boosting his likes and followers.

"The deputy's actions are deeply concerning given the number of other on-duty videos he has deleted from his TikTok account," Roberts told Ars. "Through the course of this lawsuit, we will undoubtedly uncover other instances of

livestreamed interactions with citizens between this deputy and others."

As of this writing, Castillo's TikTok account, "CycoCisco," is still active, with 17,500 followers. Ars confirmed that any videos documenting his law enforcement activity seem to have been deleted.

Dallas County Sheriff's Department did not immediately respond to Ars' request for comment but issued a statement reported by Dallas News. The department has confirmed that Castillo was suspended for two days without pay for violating the department's social media policy but remains employed by the department today. No further comments were made because the litigation is ongoing.

Osby, whose suit also names Dallas County as a defendant, has asked for a jury trial, seeking monetary relief for suffering mental and emotional anguish from the "flagrant invasion of his privacy."

TikTok declined to comment on this specific account. A spokesperson pointed Ars to TikTok's community guidelines, which prohibit sharing personally identifiable information, because TikTok acknowledges that such harassment "can cause serious emotional distress and other offline harm."

Advertisement

Osby remains "terrified" after the TikTok stream

According to Osby's complaint, the Tarrant County resident was driving to his shift at Walmart when Castillo pulled him over for allegedly speeding. Osby was surprised by the traffic stop because he claimed he was driving with cruise control on and was not speeding, but he simply continued on with his drive after Castillo let him go with just a verbal warning.

Approximately 20 minutes later, Osby found out that Castillo had livestreamed the traffic stop when Internet user “Stanley Sensational” reached out to Osby on Facebook. “Stanley” told Osby that he had found him on Facebook using the information Castillo shared on Osby’s driver’s license.

“Stanley” then shared a screenshot of Castillo’s TikTok stream, which was posted under Castillo’s account with the username “CycoCisco.” That’s when Osby learned that more than 100 of Castillo’s followers had seen the stream and thus had access to personally identifying information, including Osby’s home address, date of birth, and driver’s license number.

Osby’s lawyers have alleged that Castillo knew that Osby wasn’t speeding at the time of the traffic stop and that Castillo only pulled Osby over to make this video and spike the cop’s TikTok engagement. This allegation seemed to be backed up by an account from “Stanley,” who told Osby that on the livestream, Castillo said that he made the video just to show his followers what he does during a traffic stop.

After Osby saw the TikTok, he notified the sheriff’s department, which launched an investigation through its internal affairs department, resulting in Castillo’s brief suspension.

Since “Stanley” was able to track Osby down on Facebook, the whole experience has made Osby “terrified” that other people who saw the TikTok could use the information to track him down or steal his identity, his complaint alleges. Osby was so concerned about break-ins at his home that he installed cameras for extra security.

Among the laws that Osby alleges that Castillo broke by livestreaming the traffic stop are Osby’s constitutional rights protecting against government exposure of citizens’ private information and illegal searches and seizures. The experience also led Osby to distrust the sheriff’s department,

because his complaint said that “no reasonable officer would believe that live-streaming a police/citizen encounter on TikTok would be appropriate or necessary for the pursuit of justice, protection of life, or performance of their law enforcement duties.”

“This was not only a violation of Mr. Osby’s right to privacy but also undermines the confidence the people of Dallas County have in the law enforcement agency responsible for protecting them,” Roberts told Ars.

https://arstechnica.com/?p=1924325

FCC officials owned stock in Comcast, Charter, AT&T, and Verizon, watchdog says

Getty Images | SOPA Images

reader comments

56 with

Share this story

The Federal Communications Commission should be investigated for letting employees own stock in Comcast, Charter, AT&T, and Verizon, nonprofit watchdog group Campaign Legal Center told government officials.

“Federal law specifically bans FCC employees from owning ‘any stocks, bonds, or other securities of [any company] significantly regulated by the Commission,'” the nonprofit group said last week in a letter and detailed report sent to FCC Acting Inspector General Sharon Diskin. “Despite this ban, the most recent financial disclosures publicly available show that ethics officials allowed multiple FCC employees to own stock in telecommunications and other companies that appear to fall under the prohibition.”

The letter, sent by Campaign Legal Center General Counsel Kedric Payne and two other lawyers at the group, urged the FCC Office of Inspector General (OIG) to “investigate whether the FCC’s ethics officials took appropriate action to enforce the ethics laws… The ethics officials responsible for enforcement must explain to OIG and the public why they allowed employees to hold stocks in FCC licensed telecommunications and computer companies in apparent violation of the law.”

Citing the most recent financial disclosure reports, which cover the Chairman Ajit Pai-era years of 2018 and 2019, the Campaign Legal Center report said FCC official Rosemary Harold owned Comcast stock with a value between $3,003 and $45,000. Harold was the FCC Enforcement Bureau chief during that time and is now a deputy chief with the FCC Media Bureau. The report also said former FCC official Lisa Hone, then a deputy bureau chief, owned Charter Communications stock worth between $4,004 and $60,000.

Hone and former FCC Chief Information Security Officer Andrea Simpson owned AT&T stock, with the two employees’ AT&T holdings adding up to somewhere between $2,203 and $31,001, the report said. Harold and former Chief Technology Officer Eric Burger reportedly owned Verizon stock with a combined value between $7,007 and $105,000. The wide stock value ranges are a result of how employee stock holdings are reported in financial disclosure forms.

Advertisement

Carriers got away with false reports in 2019

The FCC has a shaky track record when it comes to punishing Internet providers. In December 2019, the FCC decided not to punish Verizon, T-Mobile, and US Cellular for exaggerating their 4G coverage in official government filings despite FCC staff writing that overstatement of "mobile broadband coverage misleads the public and can misallocate our limited universal service funds, and thus it must be met with meaningful consequences."

While the FCC chair and commissioners make the biggest policy decisions, FCC staff are responsible for investigations and play a big role in enforcement.

Our recent reporting shows that Comcast and other ISPs submitted false coverage data to the FCC's new and improved broadband map system. Comcast initially insisted the false data was accurate even after residents filed challenges at addresses where it was impossible to order Comcast Internet service. Even though Comcast didn't admit mistakes until our reporting, an FCC spokesperson told us the challenge process was working as designed.

The FCC has said there are "multiple ongoing" investigations into data submitted by ISPs, but it isn't clear whether Comcast or other providers will be punished for the false reports.

The FCC's most prominent regulatory role is in telecom, but the Campaign Legal Center also raised concerns about FCC employees owning stock in Dell, Garmin, HP, IBM, and Sony. "The FCC's laws and regulations indicate that the above-listed stocks held by FCC officials fall into two categories covered

under the stock ownership ban: telecommunications companies and FCC-licensed computer companies," the report said.

The group said it appears that all nine stocks "were held by FCC officials in violation of the Communications Act. If the FCC ethics officials issued a waiver or determined that the clear language of the regulations do not apply to the stocks, such waivers or legal analyses should be made public to help restore confidence in the ethics program of the agency." The FCC chair and ethics officials are required to enforce the laws related to employee stock ownership, the group's report said.

https://arstechnica.com/?p=1924296