Reddit mods fear spam overload as BotDefense leaves “antagonistic” Reddit

Enlarge / There could soon be much more of this on Reddit.

reader comments

67 with

The Reddit community is still reckoning with the consequences of the platform’s API price hike. The changes have led to the shuttering of numerous third-party Reddit apps and have pushed several important communities, like the Ask Me Anything (AMAs) organizers, to reduce or end their presence on the site.

The latest group to announce its departure is BotDefense. BotDefense, which helps removes rogue submission and comment bots from Reddit and which is maintained by volunteer moderators, is said to help moderate 3,650 subreddits. BotDefense’s creator told Ars Technica that the team is now quitting over Reddit’s “antagonistic actions” toward moderators and developers, with concerning implications for spam moderation on some large subreddits like r/space.

Valued bot fighter

BotDefense started in 2019 as a volunteer project and has been run by volunteer mods, known as “dequeued” and “abrownn” on Reddit. Since then, it claims to have populated its ban list with 144,926 accounts, and it helps moderate subreddits with huge followings, like r/gaming (37.4 million members), /r/aww (34.2 million), r/music (32.4 million), r/Jokes (26.2

million), r/space (23.5 million), and /r/LifeProTips (22.2 million). Dequeued told Ars that other large subreddits BotDefense helps moderates include /r/food, /r/EarthPorn, /r/DIY, and /r/mildlyinteresting.

On Wednesday, dequeued announced that BotDefense is ceasing operations. BotDefense has already stopped accepting bot account submissions and will disable future action on bots. BotDefense "will continue to review appeals and process unbans for a minimum of 90 days or until Reddit breaks the code running BotDefense," the announcement said. The announcement also advised "keeping BotDefense as a moderator through October 3rd so any future unbans can be processed."

Advertisement

The situation also highlights the importance of Pushshift, which recently lost Reddit API access due to a "miscommunication," according to Ars Technica sister site Wired—but then regained it. Pushshift is run by the Network Contagion Research Institute in Princeton, New Jersey, and is said to be popular among Reddit's thousands of volunteer moderators. As a non-commercial and educational tool, Pushshift has an exemption to Reddit's new API pricing scheme, but dequeued told Ars Technica that restrictions Reddit has imposed have "made it cumbersome to use." Further, "most of the users who submit bots to BotDefense no longer have access," the mod said.

That's important because "Pushshift is critical to our efforts to detect repost bots, comment copy bots, bots that use ChatGPT to mimic human activity, and other types of malicious bots," dequeued told Ars Technica. "Pushshift has a very detailed system for searching through past content. We use it to detect these bots. Reddit is much more limiting in searching for past posts, and the API doesn't support searching for comments."

Like other moderators Ars has spoken to, dequeued cited

shuttered third-party Reddit apps, like Apollo and RIF Is Fun, as key moderation tools. dequeued also pointed to “apps that acted as front-ends to Pushshift, which made it easier for users to research malicious accounts” as critical to BotDefense’s efforts.

Some third-party Reddit apps, like Narwhal, are still available and have moved to paid models. However, devs Ars has spoken with have shown uncertainty around how sustainable these approaches are.

Meanwhile, dequeued said that Reddit’s “few minor gestures” to keep a small number of third-party apps alive doesn’t fix the poor reputation the company now has with BotDefense.

Dequeued, who said they’ve been moderating for nearly nine years, said Reddit’s “antagonistic actions” toward devs and mods are the only reason BotDefense is closing. The moderator said there were plans for future tools, like a new machine learning system for detecting “many more” bots. Before the API battle turned ugly, dequeued had no plans to stop working on BotDefense.

https://arstechnica.com/?p=1952125

Film companies demand names of Reddit users who discussed piracy in 2011

Getty Images | natatravel

reader comments

69 with

Reddit is fighting another attempt by film companies to unmask anonymous Reddit users who discussed piracy.

The same companies lost a previous, similar motion to identify Reddit users who wrote comments in piracy-related threads. Reddit avoided revealing the identities of eight users by arguing that the First Amendment protected their right to anonymous speech.

Reddit is seeking a similar outcome in the new case, in which the film companies' subpoena to Reddit sought "Basic account information including IP address registration and logs from 1/1/2016 to present, name, email address and other account registration information" for six users who wrote comments on Reddit threads in 2011 and 2018. Reddit wrote in a court filing on Wednesday:

> *Plaintiffs' Motion seeks to unmask six anonymous Reddit users that Plaintiffs assume to have committed copyright infringement using Grande, an Internet service provider (ISP). If these Reddit users did engage in copyright infringement on Grande's networks, then Plaintiffs hope to learn whether the users were drawn to Grande for the ease of infringement. Weeks ago, this Court denied a nearly identical motion by these same Plaintiffs… But rather than returning with better facts capable of meeting the applicable First Amendment standard, Plaintiffs here offer worse facts—expressly acknowledging that they have no need to identify these Reddit users at all.*

Film companies, including Bodyguard Productions and Millennium, are behind both lawsuits. In the first case, they sued Internet provider RCN for allegedly ignoring piracy on

its broadband network. They sued Grande in the second case. Both RCN and Grande are owned by Astound Broadband.

Advertisement
Reddit is a non-party in both copyright infringement cases filed against the Astound-owned ISPs, but was served with subpoenas demanding information on Reddit users. When Reddit refused to provide all the requested information in both cases, the film companies filed motions to compel Reddit to respond to the subpoenas in US District Court for the Northern District of California.

Plaintiffs already got details on 118 users

Reddit's response to the latest motion to compel, which was previously reported by TorrentFreak today, said the film companies "have already obtained from Grande identifying information for 118 of Grande's 'top 125 pirating IP addresses.' That concession dooms the Motion; Plaintiffs cannot possibly establish that unmasking these six Reddit users is the *only* way for Plaintiffs to generate evidence necessary for their claims when they have already succeeded in pursuing an alternative and better way."

The evidence obtained directly from Grande is "far better than what they could obtain from Reddit," Reddit said, adding that plaintiffs can subpoena the 118 subscribers that are known to have engaged in copyright infringement instead.

Reddit said the six users whose identities are being sought "posted generally about using Grande to torrent. These six Reddit users responded to two threads in a subreddit for the city of Austin, Texas. The majority of the users posted over 12 years ago while the remaining two posted five years ago."

Reddit said that a "higher standard for unmasking a non-party

witness exists than for unmasking a potential defendant because—unlike the need to identify a potential defendant—litigation can often continue without trampling a non-party witness's First Amendment right to anonymity." That's one reason why the court quashed the previous subpoena to Reddit in the RCN case, the filing said:

> *In RCN, this Court recognized that the ISP "is the party that (according to the plaintiffs) 'has not reasonably implemented a policy for terminating repeat infringers,' 'controls the conduct of its subscribers,' and allows its customers 'to freely pirate without consequence.'" As a result, the Court rightly ruled that the "high likelihood that this information is available from [the ISP] defeats the plaintiffs' subpoena."*

https://arstechnica.com/?p=1952189

ChatGPT users drop for the first time as people turn to uncensored chatbots

reader comments

97 with

OpenAI's immensely popular ChatGPT has started losing users for the first time, The Washington Post reported today.

According to data firm Similarweb, ChatGPT's mobile and desktop traffic worldwide decreased by nearly 10 percent from May to June. Another data firm, Sensor Tower, reported that ChatGPT's iPhone app downloads have been steadily dipping since they peaked in early June.

This, the Post suggested, could be a sign that consumer interest in chatbots and other AI tools is waning as tech companies heavily invest in AI product development.

Earlier this year, ChatGPT set a record for attracting the fastest-growing user base in history. Many tech companies—most prominently Google—immediately sought to replicate ChatGPT's success, but Ars noted at that time that technology adoption rates have generally quickened over the past few decades. ChatGPT's success may have been less about broad interest in chatbots and more about its novelty, which may now be wearing off.

As an example that ChatGPT may have simply benefited from increasing user adoption rates, this week, Meta launched a Twitter rival called Threads. Almost instantly, Threads—despite significant drawbacks in its design and ample privacy concerns—easily beat ChatGPT's record as the fastest-growing consumer app. Where ChatGPT reached 100 million users in two months, Threads hit 70 million users in less than two days, CNBC reported. And Meta did that without depending on any flashy new AI features (in fact, Twitter has sued, alleging that Threads is just a Twitter copycat).

Advertisement

Whether a 10 percent decline in ChatGPT users over a single month in summer should worry tech companies going all in on chatbots is still unclear, though.

The Post suggested various reasons why ChatGPT might be experiencing user drop-off, including a theoretical dip in the chatbot's quality as its popularity drove up costs to keep it

running, and OpenAI attempted tweaks to lower expenses. It could even be meaningful that fewer students need to write academic papers in the summer months.

But ChatGPT has also dealt with user drama, including a recent lawsuit and an increasing number of companies urging employees not to use tools like ChatGPT out of privacy concerns, including Apple. OpenAI also started responding to user backlash and regulatory pressure by censoring harmful ChatGPT responses, which may have led some users to abandon the tool, possibly viewing it as less useful, less trustworthy, or simply less fun.

OpenAI did not immediately respond to Ars' request for comment.

https://arstechnica.com/?p=1952173

Musk's X Corp. threatens to sue Meta over Twitter "copycat" Threads

Enlarge / Mark Zuckerberg and Elon Musk.
Getty Images | AFP

reader comments

291 with

The proposed cage match between Elon Musk and Mark Zuckerberg

might never happen, but the tech titans may soon battle in a more civil arena. Musk's X Corp., the successor company to Twitter, yesterday threatened to sue Meta over alleged intellectual property violations in Meta's new Threads social network.

Musk's lawyer Alex Spiro wrote a letter on behalf of X Corp. to Meta CEO Zuckerberg. "Based on recent reports regarding your recently launched 'Threads' app, Twitter has serious concerns that Meta Platforms has engaged in systematic, willful, and unlawful misappropriation of Twitter's trade secrets and other intellectual property."

The letter was revealed today in a Semafor article. "Competition is fine, cheating is not," Musk tweeted about the letter.

Spiro claims ex-Twitter employees built Threads

Spiro's letter complains about Meta hiring some of the many workers who were laid off or resigned from Twitter in the eight months since Musk bought the company.

"Over the past year, Meta has hired dozens of former Twitter employees… these employees had and continue to have access to Twitter's trade secrets and other highly confidential information," Spiro wrote in the letter to Zuckerberg. The workers, he alleged, "owe ongoing obligations to Twitter," and many "have improperly retained Twitter documents and electronic devices."

Since taking over in late October 2022, Musk has reduced Twitter's staff from about 7,500 to about 1,500. Twitter is facing lawsuits from ex-employees over unpaid severance and bonuses.

Advertisement

Spiro's letter claimed that Meta assigned ex-Twitter "employees to develop, in a matter of months, Meta's copycat 'Threads' app with the specific intent that they use Twitter's trade secrets and other intellectual property in order to accelerate the development of Meta's competing app, in violation of both state and federal law as well as those employees' ongoing obligations to Twitter."

Meta source denies allegation

Semafor quoted a Meta source as saying that "no one on the Threads engineering team is a former Twitter employee—that's just not a thing." Spiro's letter did not say which former Twitter employees are allegedly working on Threads or specify what intellectual property is allegedly being used by Meta.

We contacted Meta and Spiro about the letter today and will update this article if we get any response.

Spiro wrote that "Twitter intends to strictly enforce its intellectual property rights, and demands that Meta take immediate steps to stop using any Twitter trade secrets or other highly confidential information." He warned that Twitter may "seek both civil remedies and injunctive relief without further notice to prevent any further retention, disclosure, or use of its intellectual property by Meta."

Spiro also suggested that Meta is violating Twitter's terms of service by scraping and crawling data from Twitter's website.

"Please consider this letter a formal notice that Meta must preserve any documents that could be relevant to a dispute between Twitter, Meta, and/or former Twitter employees who now work for Meta," Spiro wrote. That includes "all documents related to the recruitment, hiring, and onboarding of these former Twitter employees, the development of Meta's competing Threads app, and any communications between these former Twitter employees and any agent, representative, or employee

or [*sic*] Meta.”

https://arstechnica.com/?p=1952029

Threads attracts 30M users in 24 hours despite design flaws, privacy concerns

reader comments

165 with

Meta has officially launched its surprisingly popular Twitter alternative, Threads—shocking even Mark Zuckerberg as sign-ups hit 30 million within the first 24 hours. Though a separate app, Threads is built as a convenient extension of Instagram, requiring an Instagram account to join and allowing users to port their entire Instagram following over in one click. That has clearly made Threads appealing to a huge chunk of Instagram users.

“We didn’t expect tens of millions of people to sign up in one day, but supporting that is a champagne problem,” Instagram CEO Adam Mosseri said in a cheery update on Thursday.

With its well-timed launch coming just after Twitter announced unpopular rate limits on tweets, Threads has quickly surpassed ChatGPT as the fastest-growing consumer app, TechCrunch reported. But as sign-ups explode, Threads is also

experiencing immediate backlash from critics who have complained about how Threads was designed and about the app's seemingly ample privacy issues.

The most annoying thing about Threads might be that you cannot delete an account without deleting the linked Instagram account.

"You may deactivate your Threads profile at any time, but your Threads profile can only be deleted by deleting your Instagram account," the Threads Supplemental Privacy Policy says. For more details, a Meta spokesperson linked Ars to Mosseri's Threads post, which said:

> *I've been getting some questions about deleting your account. To clarify, you can deactivate your Threads account, which hides your Threads profile and content, you can set your profile to private, and you can delete individual Threads posts — all without deleting your Instagram account. Threads is powered by Instagram, so right now it's just one account, but we're looking into a way to delete your Threads account separately.*

Another big complaint is that there is no dedicated feed to see only content from accounts that users actually follow. Some users have complained that their feeds are flooded with content from accounts they never followed, seemingly outnumbering posts from friends.

In a blog post, Meta touted this default feed as a feature, saying, "Your feed on Threads includes threads posted by people you follow and recommended content from new creators you haven't discovered yet."

Since then, Mosseri and Zuckerberg have both indicated on social media that Meta could update the app in the future to provide a dedicated feed of material from accounts that users follow.

Advertisement
Other features that could be coming soon include “support for editing posts, a translation option for different languages, and options to switch between different Threads accounts,” The Verge reported. Most notably, Threads will soon be compatible with ActivityPub, which would make Threads interoperable with other apps. That would allow users to engage cross-app with others or even leave Threads and port their content and followers to other platforms. Meta’s blog, describing this decentralized approach to building an app, said:

> *We’re committed to giving you more control over your audience on Threads—our plan is to work with ActivityPub to provide you the option to stop using Threads and transfer your content to another service. Our vision is that people using compatible apps will be able to follow and interact with people on Threads without having a Threads account, and vice versa, ushering in a new era of diverse and interconnected networks.*

For now, users can control what they see by restricting who can reply to their Threads posts or mention them in replies. As on Instagram, users agree to follow the same community guidelines and can hide certain words to filter out undesirable replies. And one benefit of logging in with the same Instagram account is that Threads will ensure that any account blocked on Instagram is also blocked on Threads.

While Threads is considered part of an Instagram account, any content moderation actions that Meta takes against a Threads user will not impact their Instagram account, The Verge reported, based on a review of internal documents from Meta. However, exceptions could be made in extreme cases, like for users sharing child exploitation materials.

Privacy concerns, potential FTC scrutiny

Meta plans to keep updating the app and appears to be closely monitoring user feedback during its rollout. So far, that feedback includes privacy complaints that set Threads apart from Twitter in a seemingly less desirable way.

“All your Threads are belong to us,” Twitter co-founder Jack Dorsey tweeted, along with a screenshot showing all the sensitive data that Threads collects. Twitter owner Elon Musk amplified the tweet by responding simply, “Yeah.”

Threads collects so much sensitive data that Meta paused the app’s launch in the European Union. The company recently lost a legal fight with EU regulators, who decided that Meta can no longer claim it has a “legitimate interest” to process wide swaths of user data for advertising. Calli Schroeder, senior counsel and global privacy counsel for the Electronic Privacy Information Center (EPIC), told Ars that Threads gathers “a good amount” of data that “is not necessary for the app to function.”

Advertisement

Data collected by Threads can include users’ sexual orientation, race and ethnicity, biometric data, trade union membership, pregnancy status, politics, and religious beliefs. Threads can also collect data on users’ employment, as well as health and fitness. Beyond that, the app also can collect data monitoring users’ location and other web activity.

“Health and financial data, precise location, search history, browsing history, and more are not needed for a user to be on the app and are instead used to create a more hyper-personalized and targeted experience on the app or shared with and sold to advertisers,” Schroeder told Ars.

All of these privacy concerns are red flags in the EU, where

users must give consent before sensitive data can be collected, Quartz reported. Schroeder said that the concerns could also be considered red flags by users anywhere who are aware of Meta's "history of concerning privacy practices" and who might otherwise choose to opt out of such extensive data collection. Because of these concerns, it's possible that Threads will never be offered in the EU, TechCrunch reported.

"Incoming EU regulations entirely bar using sensitive data for ads," Schroeder told Ars, in reference to the Digital Markets Act.

Meta may run into trouble with Threads in the US, too, Schroeder said. Meta is currently under a consent decree from the US Federal Trade Commission (FTC), under which it's possible that Meta's decision to link Threads accounts to Instagram accounts could be considered a violation or an "unfair or deceptive" practice because it potentially obscures what steps a user must take to control their data.

"It looks like Threads automatically links with a user's Instagram account and a user can't delete Threads without also deleting the Instagram," Schroeder told Ars. "This may violate Meta's consent order with the FTC, which bars Meta from misrepresenting the privacy or security of covered data, including the extent to which a consumer can control the privacy of the information and the steps they have to take to maintain control."

Of all the Twitter alternatives popping up, Schroeder cautioned that Threads may have the most privacy concerns.

"Threads is one of the most privacy-invasive options we've seen," Schroeder told Ars. "Users wanting to ditch Twitter can absolutely still do so but may have to pick a better alternative than Threads (and consider whether they want to trust Elon *or* Zuckerberg with their personal data)."

In a Threads post, Zuckerberg took a light jab at Twitter

while optimistically predicting that Threads could become the first online public square that attracts a billion users—which was Musk's target for Twitter to hit by 2024.

"I think there should be a public conversations app with 1 billion+ people on it," Zuckerberg posted on Threads. "Twitter has had the opportunity to do this but hasn't nailed it. Hopefully we will."

https://arstechnica.com/?p=1951976

State Dept. cancels election meetings with Facebook after "free speech" ruling

Enlarge / US President Joe Biden exits the White House before boarding Marine One on Thursday, July 6, 2023.
Getty Images | Bloomberg

reader comments

87 with

The Biden administration is appealing a federal judge's ruling that ordered the government to halt a wide range of communications with social media companies. President Biden and the other federal defendants in the case "hereby appeal" the ruling to the US Court of Appeals for the Fifth Circuit, according to a notice filed in US District Court yesterday. The US will submit a longer filing with arguments to the 5th

Circuit appeals court.

On Tuesday, Judge Terry Doughty of US District Court for the Western District of Louisiana granted a preliminary injunction that prohibits White House officials and numerous federal agencies from communicating “with social-media companies for the purpose of urging, encouraging, pressuring, or inducing in any manner the removal, deletion, suppression, or reduction of content containing protected free speech posted on social-media platforms.”

Doughty found that defendants “significantly encouraged” and in some cases coerced “the social-media companies to such extent that the decision [to modify or suppress content] should be deemed to be the decisions of the Government.” The Biden administration has argued that its communications with tech companies are permissible under the First Amendment and vital to counter misinformation about elections, COVID-19, and vaccines.

Department of Justice lawyers are expected to seek a stay of the preliminary injunction. The 5th Circuit court that will handle the Biden appeal last year upheld a Texas law that prohibits social media companies from moderating content based on a user’s “viewpoint.”

State Dept. cancels Facebook meetings

In the meantime, the Biden administration is taking steps to avoid violating Doughty’s injunction. According to The Washington Post, “the State Department canceled its regular meeting Wednesday with Facebook officials to discuss 2024 election preparations and hacking threats.”

“State Department officials told Facebook that all future meetings, which had been held monthly, have been ‘canceled

pending further guidance,'" the Post wrote, citing a source at Facebook.

Doughty, a Trump nominee, made the ruling in a lawsuit filed by the Missouri and Louisiana attorneys general. Doughty ruled that plaintiffs "are likely to succeed on the merits on their claim that the United States Government, through the White House and numerous federal agencies, pressured and encouraged social-media companies to suppress free speech."

Advertisement

The injunction doesn't cut off all contact between the Biden administration and social media companies. Doughty's ruling said the government may continue to inform social networks about posts involving criminal activity or criminal conspiracies, national security threats, extortion, criminal efforts to suppress voting, illegal campaign contributions, cyberattacks against election infrastructure, foreign attempts to influence elections, threats to public safety and security, and posts intending to mislead voters about voting requirements and procedures.

The US can also exercise "permissible public government speech promoting government policies or views on matters of public concern," communicate with social networks "in an effort to detect, prevent, or mitigate malicious cyber activity," and "communicat[e] with social-media companies about deleting, removing, suppressing, or reducing posts on social-media platforms that are not protected free speech by the Free Speech Clause in the First Amendment to the United States Constitution."

Election disinformation talks expected to continue

The Washington Post paraphrased a Homeland Security official as saying that "many of the activities they pursued, such as

warnings about election disinformation, are exempted from the injunction and are likely to continue."

State Department meetings with Facebook and other tech companies are used to discuss foreign influence operations, the Post wrote. One person who is familiar with the talks told the news organization that "State will share Russian narratives, things they are seeing in state media in Russia about US topics. They will ask whether Facebook is seeing things from known entities, such as the Chinese Communist Party or the Internet Research Agency." The Internet Research Agency is a Russian company charged with seeking to interfere in the 2016 US presidential election.

White House Press Secretary Karine Jean-Pierre said in a press briefing yesterday that "DOJ is reviewing the injunction" and that "we disagree with the decision."

"We are going to continue to promote responsible actions to protect public health, safety, and security when confronted by challenges like a deadly pandemic and foreign attacks on our election… Our view remains that social media platforms have a critical responsibility to take action or to take account of the effects of their platforms are having to the American people but make independent choices about the information they present," Jean-Pierre said.

In addition to the Missouri and Louisiana attorneys general, the plaintiffs in the case against the Biden administration include professors Jayanta Bhattacharya and Martin Kulldorff, who co-authored the October 2020 "Great Barrington Declaration" that opposed COVID lockdowns and urged a focus on reaching herd immunity. Robert F. Kennedy Jr. and his anti-vaccine Children's Health Defense group, which was banned from Facebook for violating COVID-19 policies, are trying to have their own lawsuit against Biden consolidated with the Missouri/Louisiana case.

https://arstechnica.com/?p=1951942

Judge rules White House pressured social networks to “suppress free speech”

Getty Images | Christopher Furlong

reader comments

260 with

A federal judge yesterday ordered the Biden administration to halt a wide range of communications with social media companies, siding with Missouri and Louisiana in a lawsuit that alleges Biden and his administration violated the First Amendment by colluding with social networks “to suppress disfavored speakers, viewpoints, and content.”

The Biden administration argued that it communicated with tech companies to counter misinformation related to elections, COVID-19, and vaccines, and that it didn’t exert illegal pressure on the companies. The communications to social media companies were not significant enough “to convert private conduct into government conduct,” Department of Justice lawyers argued in the case.

But Judge Terry Doughty, a Trump nominee at US District Court for the Western District of Louisiana, granted the plaintiffs’ request for a preliminary injunction imposing limits on the

Department of Health and Human Services, the National Institute of Allergy and Infectious Diseases, the Centers for Disease Control and Prevention, the Federal Bureau of Investigation, the Department of Justice, the US Census Bureau, the State Department, the Homeland Security Department, the Cybersecurity and Infrastructure Security Agency, and many specific officials at those agencies. The injunction also affects White House officials.

The agencies and officials are prohibited from communicating "with social-media companies for the purpose of urging, encouraging, pressuring, or inducing in any manner the removal, deletion, suppression, or reduction of content containing protected free speech posted on social-media platforms," Doughty ruled. The injunction prohibits "specifically flagging content or posts on social-media platforms and/or forwarding such to social-media companies urging, encouraging, pressuring, or inducing in any manner for removal, deletion, suppression, or reduction of content containing protected free speech."

Advertisement

Government agencies and officials are further barred from urging, encouraging, or pressuring social media companies "to change their guidelines for removing, deleting, suppressing, or reducing content containing protected free speech." The ruling also said the government may not coordinate with third-party groups, including the Election Integrity Partnership, the Virality Project, and the Stanford Internet Observatory, to pressure social media companies.

Exceptions include voting misinformation

Doughty provided several exceptions that allow the government to communicate with social media companies about criminal activity and other speech that the First Amendment doesn't

protect. The Biden administration may continue to inform social networks about posts involving criminal activity or criminal conspiracies, national security threats, extortion, criminal efforts to suppress voting, illegal campaign contributions, cyberattacks against election infrastructure, foreign attempts to influence elections, threats to public safety and security, and posts intending to mislead voters about voting requirements and procedures.

The US can also exercise "permissible public government speech promoting government policies or views on matters of public concern," communicate with social networks "in an effort to detect, prevent, or mitigate malicious cyber activity," and "communicat[e] with social-media companies about deleting, removing, suppressing, or reducing posts on social-media platforms that are not protected free speech by the Free Speech Clause in the First Amendment to the United States Constitution."

In addition to the Missouri and Louisiana attorneys general, the plaintiffs include professors Jayanta Bhattacharya and Martin Kulldorff, who co-authored the October 2020 "Great Barrington Declaration" that opposed COVID lockdowns and urged a focus on reaching herd immunity. They and other plaintiffs claim they were censored by social networks.

The ruling was criticized by Jameel Jaffer, an adjunct professor of law and journalism who is executive director of the Knight First Amendment Institute at Columbia University. "It can't be that the government violates the First Amendment simply by engaging with the platforms about their content-moderation decisions and policies," Jaffer told The New York Times, calling it "a pretty radical proposition that isn't supported by the case law."

Advertisement

While the government must be careful to avoid coercion in its efforts to combat false information, Jaffer said that

“unfortunately, Judge Doughty’s order doesn’t reflect a serious effort to reconcile the competing principles.”

Stanford Law School Assistant Professor Evelyn Douek told The Washington Post that the “injunction is strikingly broad and clearly intended to chill any kind of contact between government actors and social media platforms.”

Judge finds “unrelenting pressure” on social networks

Doughty previously blocked federal vaccine and mask mandates in the Head Start program. In the social media case, Doughty made it clear that he expects plaintiffs to win in a 155-page memorandum ruling explaining his decision yesterday:

> *The Plaintiffs are likely to succeed on the merits on their claim that the United States Government, through the White House and numerous federal agencies, pressured and encouraged social-media companies to suppress free speech. Defendants used meetings and communications with social-media companies to pressure those companies to take down, reduce, and suppress the free speech of American citizens.*
>
> *They flagged posts and provided information on the type of posts they wanted suppressed. They also followed up with directives to the social-media companies to provide them with information as to action the company had taken with regard to the flagged post. This seemingly unrelenting pressure by Defendants had the intended result of suppressing millions of protected free speech postings by American citizens.*

The federal defendants “argue they only made requests to the social-media companies, and that the decision to modify or suppress content was each social-media company’s independent decision,” Doughty wrote. “However, when a state has so involved itself in the private party’s conduct, it cannot

claim the conduct occurred as a result of private choice, even if the private party would have acted independently."

He found that defendants "significantly encouraged" and in some cases coerced "the social-media companies to such extent that the decision should be deemed to be the decisions of the Government."

https://arstechnica.com/?p=1951745

Generative AI in games will create a copyright crisis

reader comments

66 with

AI Dungeon, a text-based fantasy simulation that runs on OpenAI's GPT-3, has been churning out weird tales since May 2019. Reminiscent of early text adventure games like *Colossal Cave Adventure*, you get to choose from a roster of formulaic settings—fantasy, mystery, apocalyptic, cyberpunk, zombies—before picking a character class and name, and generating a story.

Here was mine: "You are Mr. Magoo, a survivor trying to survive in a post-apocalyptic world by scavenging among the ruins of what is left. You have a backpack and a canteen. You haven't eaten in two days, so you're desperately searching for food." So began Magoo's 300-ish-word tale of woe in which,

“driven half-mad” by starvation, he happens upon “a man dressed in white.” (Jesus? Gordon Ramsay?) Offering him a greeting kiss, Magoo is stabbed in the neck.

As lame as this story is, it hints at a knotty copyright issue the games industry is only just beginning to unravel. I’ve created a story using my imagination—but to do that I’ve used an AI helper. So who wrote the tale? And who gets paid for the work?

AI Dungeon was created by Nick Walton, a former researcher at a deep learning lab at Brigham Young University in Utah who is now the CEO of Latitude, a company that bills itself as “the future of AI-generated games.” *AI Dungeon* is certainly not a mainstream title, though it has still attracted millions of players. As Magoo’s tale shows, the player propels the story with action, dialog, and descriptions; *AI Dungeon* reacts with text, like a dungeon master—or a kind of fantasy improv.

Advertisement

In several years of experimentation with the tool, people have generated far more compelling D&D-esque narratives than mine, as well as videos like “I broke the AI in *AI Dungeon* with my horrible writing.” It’s also conjured controversy, notably when users began prompting it to make sexually explicit content involving children. And as *AI Dungeon*—and tools like it—evolve, they will raise more difficult questions about authorship, ownership, and copyright.

Many games give you toolsets to create worlds. Classic series like *Halo* or *Age of Empires* include sophisticated mapmakers; *Minecraft* precipitated an open-ended, imaginative form of gameplay that *The Legend of Zelda: Tears of the Kingdom*’s Fuse and Ultrahand capabilities draw clear inspiration from; others, like *Dreams* or *Roblox*, are less games than platforms for players to make more games.

Historically, claims of ownership to in-game creations or user-generated creations (IGCs or UGCs) have been rendered moot by “take it or leave it” end-user license agreements—the dreaded EULAs that nobody reads. Generally, this means players surrender any ownership of their creations by switching on the game. (*Minecraft* is a rare exception here. Its EULA has long afforded players ownership of their IGCs, with relatively few community freakouts.)

AI adds new complexities. Laws in both the US and the UK stipulate that, when it comes to copyright, only humans can claim authorship. So for a game like *AI Dungeon*, where the platform allows a player to, essentially, “write” a narrative with the help of a chatbot, claims of ownership can get murky: Who owns the output? The company that developed the AI, or the user?

There’s a big discussion nowadays, with prompt engineering in particular, about the extent to which you as a player imprint your personality and your free and creative choices,” says Alina Trapova, a law professor at University College London who specializes in AI and copyright and has authored several papers on *AI Dungeon’s* copyright problems. Right now, this gray area is circumvented with an EULA. *AI Dungeon*’s is particularly vague. It states that users can use content they create “pretty much however they want.” When I emailed Latitude to ask whether I could turn my Mr. Magoo nightmare into a play, book, or film, the support line quickly responded, “Yes, you have complete ownership of any content you created using *AI Dungeon*.”

https://arstechnica.com/?p=1951703

Pornhub cuts off more US users in ongoing protest over age-verification laws

reader comments

166 with

On July 1, laws requiring adult websites to verify user ages took effect in Mississippi and Virginia, despite efforts by Pornhub to push back against the legislation. Those efforts include Pornhub blocking access to users in these states and rallying users to help persuade lawmakers that requiring ID to access adult content will only create more harm for users in their states.

Pornhub posted a long statement on Twitter, explaining that the company thinks US officials acting to prevent children from accessing adult content is “great.” However, “the way many elected officials have chosen to implement these laws is haphazard and dangerous.”

Pornhub isn’t the only one protesting these laws. Last month, the Free Speech Coalition (FSC) sued Louisiana over its age-verification law, with FSC Executive Director Alison Boden alleging that these kinds of laws now passed in seven states are unconstitutional.

“These laws give the state the power to harass and censor legal businesses,” Boden said in a blog. “We, of course, support keeping minors from accessing adult content, but allowing the state to suppress certain speech by requiring

invasive and burdensome systems that consumers refuse to engage with is simply state censorship."

Just before the Mississippi and Virginia laws took effect, the FSC confirmed in another blog that it is "looking at potential challenges to these laws."

Ars could not immediately reach Pornhub or the FSC for comment. [**Update:** FSC director of public affairs, Mike Stabile, told Ars that there will likely be an update later this week regarding FSC legal challenges in states passing age verification laws. Stabile said that "it's important to understand that these laws are less about protecting minors, and more about restricting the open Internet. State-level regulations that primarily target adult sites are tremendously ineffective at keeping minors from accessing adult content." Stabile said these regulations are also dangerous because they are "just the beginning of the speech the government is hoping to limit, which is why it's so important to fight it now."

Advertisement
"We're in the midst of twin moral panics around sex and tech, and porn is where they overlap," Stabile told Ars. He noted that "laws affect much more than adult sites" because of vague language that makes it so things like "a 'description of a female nipple' is enough to trigger liability" in some states for various other websites, including sex education resources. Stabile said that FSC advocates for device-based age verification that is "a far better option for keeping minors from accessing adult content."]

In its Twitter statement, Pornhub alleged that a major problem with these laws is that states "are not regulating enforcement." This means that major platforms like Pornhub will likely comply with the laws voluntarily—or else risk fines of up to $1 million annually, the FSC estimated—while users seeking to avoid age verification will simply migrate over to seedier platforms that don't require ID and often pose

security and privacy risks to users.

Pornhub has said that rather than requiring platforms to ask for ID, lawmakers should require device-based age verification as "the only solution that makes the Internet safer."

Users skirting age verification

According to the FSC's age verification law tracker, laws in three more states are scheduled to take effect in the near future. Arkansas will be next, with its law taking effect on July 31, Texas on September 1, and Montana on January 1, 2024.

Until a better solution is found, Pornhub—which SimilarWeb currently ranks as the eighth most-visited website in the US—seems likely to continue blocking access to more and more US users. It seems to be Pornhub's only real way to protest the laws and force lawmakers to consider their concerns over what Pornhub views as misguided age-verification laws. In Utah, at least one lawmaker, Todd Weiler, told Ars that he was shocked that Pornhub would take such a drastic step.

Advertisement
Pornhub has apologized to "loyal visitors" whose access has now been blocked in increasingly more states, but many users have found that it's pretty easy to skirt age verification and Pornhub's block by using a VPN. This weekend, Google Trends data showed that "VPN" quickly became a top search term for Virginia Internet users.

The FSC seemed to back sites like Pornhub choosing to block access in these states rather than complying with age-verification laws. Similar to Pornhub's online campaign to rally users to push back against lawmakers, the FSC launched a website, Defend Online Privacy. It's a resource providing landing pages to help websites like Pornhub easily redirect newly blocked users. Instead of loading Pornhub's homepage, a Pornhub user would theoretically be redirected to a landing

page designed to raise awareness for users in Arkansas, Louisiana, Mississippi, Montana, Texas, Utah, and Virginia, explaining “why they’re being blocked” and encouraging them “to contact the legislators in that state to express their displeasure with the law.”

The plan is to inform Internet users, who can then influence local lawmakers like Weiler, who previously told Ars that he didn’t think requiring ID to access adult content was “too much to ask.” To him, it seemed just like requiring a cashier to ask for ID before selling anyone alcohol or cigarettes.

But the FSC’s New Orleans-based counsel Jeff Sandman said in a blog post that there’s an obvious reason why this comparison is not appropriate, and some lawmakers are overlooking it.

“The First Amendment protects our right to freely access legal content and ideas without government interference,” Sandman said. “We’re fighting not only for adult businesses but for the right of legal adults to use the Internet without government surveillance. Showing your ID in a checkout lane is simply not the same as submitting it to a government database.”

In Louisiana, FSC lawyers have asked a judge to block the state from enforcing its law, and it seems likely that the FSC will make the same demands in Mississippi and Virginia.

https://arstechnica.com/?p=1951582

Musk annoys Twitter users by

capping number of tweets they can view each day

Getty Images | NurPhoto

reader comments

338 with

Twitter has imposed limits on how many tweets users can view each day, with owner Elon Musk claiming the drastic change was needed to fight “data scraping” and other “manipulation.” Users who hit the rate limits were greeted with error messages like “Sorry, you are rate limited. Please wait a few moments then try again.”

“To address extreme levels of data scraping & system manipulation, we’ve applied the following temporary limits: – Verified accounts are limited to reading 6000 posts/day – Unverified accounts to 600 posts/day – New unverified accounts to 300/day,” Musk wrote on Saturday.

When Musk says “verified,” of course, he means users who pay $8 a month for the Twitter Blue subscription that comes with certain perks, such as adding a blue checkmark to the accounts of subscribers. Prior to Musk’s ownership of Twitter, “verified” meant that a user had been confirmed to be notable and authentic.

Musk said later that rate limits would soon rise “to 8000 for verified, 800 for unverified & 400 for new unverified.” A third Musk tweet on Saturday afternoon suggested that the limits had been raised to 10,000 for Twitter Blue subscribers, 1,000 for most other accounts, and 500 for new accounts that

aren’t paying for a subscription.

The rate limits were widely mocked by Twitter users all weekend, as trending topics included “#RateLimitExceeded” and “#RIPTwitter.” Musk seemed unconcerned, writing, “Oh the irony of hitting view limits due to complaining about view limits.”

Massive staff cuts make fixing problems harder

While Musk suggested that he was forced to limit Twitter usage, the extreme staff cuts he’s imposed have likely made it harder for Twitter to solve problems without affecting the user experience. Since he bought the social network in October 2022, Musk’s cost-cutting has reduced Twitter’s staff from about 7,500 to about 1,500.

Advertisement
In March, a single engineer’s mistake essentially broke the Twitter API, causing an outage that broke links and other functionality for about an hour. Because of the staff cuts, “every mistake in code and operations is now deadly,” one former engineer told The Washington Post in November.

While the latest problems happened shortly after Twitter reportedly stopped paying its bills for Google Cloud services, Twitter already resumed payments to Google before the rate limits were imposed.

In another change, Twitter also now requires people to be logged in to view tweets or profiles. Previously, you could view a tweet or a person’s account without logging into a Twitter account. “Temporary emergency measure,” Musk wrote on Friday to explain the change. “We were getting data pillaged so much that it was degrading service for normal users!”

Former Twitter executive Yoel Roth didn’t buy Musk’s explanation. “It just doesn’t pass the sniff test that

scraping all of a sudden created such dramatic performance problems that Twitter had no choice but to put everything behind a login," Roth wrote in a post on Twitter rival Bluesky. "Scraping was the open secret of Twitter data access. We knew about it. It was fine."

Roth was Twitter's head of trust and safety for seven years before resigning on November 10 over objections to what he called Musk's "dictatorial" leadership style. Roth also commented on Twitter's new policy of charging for API access. "Old management, for all its flaws, recognized that Twitter data was fundamentally public," Roth wrote Saturday. "We could sell access to APIs that made it easier or better to work with—but undermining the publicness of the service to squeeze a little more cash out of the data licensing business was just never practical."

https://arstechnica.com/?p=1951560