X “unfit” for banking because of complicity in Saudi spying, lawyers argue

reader comments

138 with

Just two weeks after Elon Musk took over Twitter in fall 2022, he told employees that his big plan to save the social media platform from bankruptcy was to turn it into a bank. Since then, he has rebranded the platform as X, and banking regulators in eight US states have approved his applications for money-transmitting licenses.

Now, as X continues filing for money-transmitting licenses—in pursuit of turning X into an “everything app,” a one-stop destination where users bank, shop, communicate, and basically spend all their time online—US banking regulators are being urged to reconsider approving X’s applications to provide financial services, The Guardian reported. And Ars confirmed that states that already granted licenses are being pressured to revoke them.

In an open letter reviewed by Ars, lawyers at Walden Macht & Haran LLP—who are representing a Saudi family suing Twitter/X—warned both “attorneys general and banking commissioners across 50 states” that Musk’s company should be considered “unfit” to hold banking licenses. They alleged that X is unfit for banking due to its alleged treatment of users’ personal data and “intentional complicity” in human rights violations. These grievances, The Guardian reported, also

call into question whether X “can be trusted to abide by federal and state laws protecting consumer data and records.”

That particular lawsuit against Twitter was initially filed in May, alleging that former Twitter employees—who were charged in 2019 with conspiring with the Saudi regime to silence more than 6,000 dissidents—violated Twitter’s terms of service by unmasking anonymous Twitter accounts run by Saudi users like human rights activist Abdulrahman Al-Sadhan. After Twitter’s employees identified Al-Sadhan to the Saudi government, Twitter allegedly never notified him before he was reportedly kidnapped, tortured, and imprisoned in 2021—sentenced to 20 years for posting tweets mocking the royal family.

Advertisement
His sister, Areej, sued Twitter on behalf of her brother, accusing Twitter of looking the other way after the FBI notified Twitter of the suspected employee spying. The lawsuit argued that Twitter violated its own ToS by sharing Al-Sadhan’s account information, allegedly because the company was financially motivated not to rile the Saudi government. An amended complaint in the lawsuit filed last week noted that Al-Sadhan’s family has been denied contact with Al-Sadhan and “is not sure if he is alive.”

Areej’s complaint also noted that the Kingdom of Saudi Arabia (KSA) is Twitter/X’s most important market in the Middle East, and the open letter noted that Musk knew about the spying and still allowed Saudi investors to become the second largest stakeholders in the platform.

X has not yet commented on the letter or responded to Areej’s amended complaint. But as experts predicted, the company has argued that it was also a victim of its employees’ covert spying.

The open letter disputed that defense, claiming that “compelling” evidence shows that Twitter was not a victim. The

letter alleged that as proof of the platform's complicity, instead of cracking down on Saudi spying after the FBI alert, "Twitter began approving Saudi requests for confidential information, including 'emergency disclosures,' in 'droves.'"

"In 2016, 85 percent of all information requests were approved, eclipsing approval rates for Canada and the United Kingdom," the letter said. "While Twitter has protested that it was a 'victim' of its employees' misconduct, the evidence we found tells a much different story—one in which a financially troubled Twitter essentially sold its corporate soul to secure KSA's investment in Twitter and to ensure Twitter remained available in KSA, one of Twitter's largest markets (while countries such as Turkey banned it)."

While the employee spying happened well before Musk bought Twitter, Al-Sadhan's lawyers told US regulators this week that "X's prior and current conduct deserves 'serious and careful investigation.'" If there is no investigation, lawyers allege that the KSA could gain unprecedented access to users' confidential financial information. They've alleged that the stakes are high because X has "acted at the direction of Saudi Arabia in furtherance of the kingdom's campaign of transnational repression."

https://arstechnica.com/?p=1966584

4th FTX exec pleads guilty, agrees to forfeit Porsche and

other property

Enlarge / Ryan Salame, former co-chief executive officer of FTX Digital Markets Ltd., exits federal court in New York on Thursday, Sept. 7, 2023.
Getty Images | Bloomberg

reader comments

55 with

Former FTX executive Ryan Salame pleaded guilty to two criminal charges yesterday, becoming the fourth former associate of Sam Bankman-Fried to enter guilty pleas.

A money judgment of $1.56 billion was entered against Salame, but he will be allowed to satisfy the judgment by making a $6 million payment to the US and forfeiting two properties, a business, and a Porsche. He also agreed to provide $5.6 million in restitution to FTX debtors.

Salame faces a maximum imprisonment of 10 years, consisting of five years for each charge. Salame was released on a $1 million bond and has sentencing scheduled for March 6, 2024. Meanwhile, Bankman-Fried's trial is scheduled to begin in early October.

Salame joined FTX affiliate Alameda in 2019 and was named co-CEO of FTX's Bahamian affiliate FTX Digital Markets in October 2021, according to a charging document filed in US District Court for the Southern District of New York. Salame pleaded guilty to conspiracy to make unlawful political contributions and defraud the Federal Election Commission, and conspiracy to operate an unlicensed money-transmitting business.

"I made political contributions in my name that were funded by

transfers from an Alameda subsidiary," Salame told Judge Lewis Kaplan as he pleaded guilty, according to a CoinDesk article. The donations "were for the benefit of initiatives introduced by others but supported by Sam Bankman-Fried," Salame was quoted as saying.

Advertisement
The transfers to Salame were categorized as loans. "I understood that the loans would eventually be forgiven, and that I would never have to repay them," Salame said in court, according to a New York Times article.

Substitute assets

Salame agreed to forfeit a 2021 Porsche 911 Turbo S and two properties in Lenox, Massachusetts. One of the properties is the site of a restaurant called the Olde Heritage Tavern.

Salame also agreed to give up ownership and equity interest in the Olde Heritage Tavern business. Before the downfall of cryptocurrency exchange FTX, Salame made "multi-million dollar investments in downtown Lenox restaurants and real estate," a Berkshire Eagle article in November 2022 said.

The $1.56 billion judgment against Salame represents the amount involved in the criminal charge for conspiracy to operate an unlicensed money-transmitting business, according to a forfeiture order filed yesterday. The US agreed to accept a $6 million payment and "substitute assets" instead of the full $1.56 billion judgment. The US can pursue the entire $1.56 billion judgment if Salame fails to make the payment or forfeit the assets, or if he submitted false or incomplete information in his financial affidavit.

There was previously speculation that Salame would agree to give up a private jet. A Bloomberg report last month said that the "plane could potentially be forfeited as part of a plea deal with the government or clawed back for creditors in the

company’s bankruptcy proceedings.”

https://arstechnica.com/?p=1966684

The International Criminal Court will now prosecute cyberwar crimes

Enlarge / Karim Khan speaks at Colombia’s Special Jurisdiction for Peace during the visit of the Prosecutor of the International Criminal Court in Bogota, Colombia, on June 6, 2023.

reader comments

19 with

For years, some cybersecurity defenders and advocates have called for a kind of Geneva Convention for cyberwar, new international laws that would create clear consequences for anyone hacking civilian critical infrastructure, like power grids, banks, and hospitals. Now the lead prosecutor of the International Criminal Court at the Hague has made it clear that he intends to enforce those consequences—no new Geneva Convention required. Instead, he has explicitly stated for the first time that the Hague will investigate and prosecute any hacking crimes that violate existing international law, just as it does for war crimes committed in the physical world.

In a little-noticed article released last month in the

quarterly publication Foreign Policy Analytics, the International Criminal Court's lead prosecutor, Karim Khan, spelled out that new commitment: His office will investigate cybercrimes that potentially violate the Rome Statute, the treaty that defines the court's authority to prosecute illegal acts, including war crimes, crimes against humanity, and genocide.

"Cyberwarfare does not play out in the abstract. Rather, it can have a profound impact on people's lives," Khan writes. "Attempts to impact critical infrastructure such as medical facilities or control systems for power generation may result in immediate consequences for many, particularly the most vulnerable. Consequently, as part of its investigations, my Office will collect and review evidence of such conduct."

When WIRED reached out to the International Criminal Court, a spokesperson for the office of the prosecutor confirmed that this is now the office's official stance. "The Office considers that, in appropriate circumstances, conduct in cyberspace may potentially amount to war crimes, crimes against humanity, genocide, and/or the crime of aggression," the spokesperson writes, "and that such conduct may potentially be prosecuted before the Court where the case is sufficiently grave."

Advertisement

Neither Khan's article nor his office's statement to WIRED mention Russia or Ukraine. But the new statement of the ICC prosecutor's intent to investigate and prosecute hacking crimes comes in the midst of growing international focus on Russia's cyberattacks targeting Ukraine both before and after its full-blown invasion of its neighbor in early 2022. In March of last year, the Human Rights Center at UC Berkeley's School of Law sent a formal request to the ICC prosecutor's

office urging it to consider war crime prosecutions of Russian hackers for their cyberattacks in Ukraine—even as the prosecutors continued to gather evidence of more traditional, physical war crimes that Russia has carried out in its invasion.

In the Berkeley Human Rights Center's request, formally known as an Article 15 document, the Human Rights Center focused on cyberattacks carried out by a Russian group known as Sandworm, a unit within Russia's GRU military intelligence agency. Since 2014, the GRU and Sandworm, in particular, have carried out a series of cyberwar attacks against civilian critical infrastructure in Ukraine beyond anything seen in the history of the internet. Their brazen hacking has ranged from targeting Ukrainian electric utilities and triggering the only two blackouts ever caused by cyberattacks to the release of the data-destroying NotPetya malware that spread from Ukraine to the rest of the world and inflicted more than $10 billion in damage, including to hospital networks in both Ukraine and the United States.

Though the Berkeley group's submission initially focused on Sandworm's 2015 and 2016 attacks on Ukraine's power grid as the clearest example of cyberattacks with physical effects comparable to those of traditional warfare, it later expanded its argument to include Sandworm's NotPetya cyberattack, as well as a third attempt by the hackers to sabotage Ukraine's power grid and another cyberattack on the Viasat satellite modem network used by Ukraine's military, which caused outages of the satellite modems across Europe.

https://arstechnica.com/?p=1966589

Musk calling shots on X content explains advertiser exodus, former exec says

reader comments

148 with

Recently, Elon Musk has made it clear that he blames advocates speaking out about hate speech for plummeting ad revenue on X, the platform formerly known as Twitter. But today, Reuters published an exclusive interview with a former Twitter ad exec, AJ Brown, who seemed to push back on Musk's narrative.

The platform's former head of brand safety and ad quality suggested that X advertisers aren't just pulling back as a knee-jerk reaction to critics' claims that the platform has become increasingly toxic under Musk. Brown told Reuters that X shifting its content moderation policy to "limiting reach" of offensive content—rather than removing the content—"made it challenging to convince brands" that Musk's social media platform "was safe for ads."

"Helping people wrap their minds around the concept that violating a policy would no longer result in the removal of whatever was violating the policy, was a difficult message to communicate to people," Brown told Reuters.

This suggests that for some advertisers, it's not necessarily the amount of hate speech that's the problem, but is instead even the remote possibility that their brand's ads could be displayed next to offensive content that has them pausing ad

campaigns. To brands, it’s seemingly all about what X is doing to ensure brand safety, and for major brands, the answer to that question at various times has been: not enough.

To anyone closely following Musk’s reign at Twitter/X, these insights that Brown shared with Reuters is not news but rather a reminder of what advertisers have been saying since Musk took over the platform.

Advertisement
In November, when 14 of then-Twitter’s top advertisers had left the platform, one of those brands, Mars, released a statement that the company suspended ads because of “significant brand safety and suitability incidents.” An advertiser-led group, the Global Alliance for Responsible Media, warned Musk that “brand safety is non-negotiable for advertisers,” and though X has reported that 99 percent of content views are of “healthy” posts, it’s obvious that limiting reach isn’t a perfect strategy. Just last month, X suspended a pro-Hitler account when two brands suspended advertising after Media Matters shared screenshots of their ads being displayed on the violative account’s feed.

After last month’s incident, X announced that the platform was adding more brand safety controls to assuage advertisers’ fears. Now advertisers can block ads from appearing next to posts containing certain keywords. They can also adjust “sensitivity settings” to mark their accounts as ‘conservative’ and avoid ad placements next to “targeted hate speech, explicit sexual content, gratuitous gore, excessive profanity, obscenity, spam, drugs.”

“Your ads will only air next to content that is appropriate for you,” Yaccarino told CNBC.

For six years, it was Brown’s job to make sure that nobody’s ads appeared next to unsuitable content, Brown told Reuters. He said as soon as Musk came on board, advertisers started

voicing concerns, “fearful” of ads appearing next to harmful posts. When Musk changed the content moderation policy to “Freedom of Speech, Not Reach” last April, Brown said that only raised more questions for advertisers who had already paused spending and weren’t convinced that the policy change was a positive development.

Media Matters Vice President Julie Millican told Ars that the nonprofit watchdog group will continue to monitor X to document instances of ads being displayed next to harmful posts.

https://arstechnica.com/?p=1966250

AI-generated child sex imagery has every US attorney general calling for action

reader comments

174 with

On Wednesday, American attorneys general from all 50 states and four territories sent a letter to Congress urging lawmakers to establish an expert commission to study how generative AI can be used to exploit children through child sexual abuse material (CSAM). They also call for expanding existing laws against CSAM to explicitly cover AI-generated

materials.

“As Attorneys General of our respective States and territories, we have a deep and grave concern for the safety of the children within our respective jurisdictions,” the letter reads. “And while Internet crimes against children are already being actively prosecuted, we are concerned that AI is creating a new frontier for abuse that makes such prosecution more difficult.”

In particular, open source image synthesis technologies such as Stable Diffusion allow the creation of AI-generated pornography with ease, and a large community has formed around tools and add-ons that enhance this ability. Since these AI models are openly available and often run locally, there are sometimes no guardrails preventing someone from creating sexualized images of children, and that has rung alarm bells among the nation’s top prosecutors. (It’s worth noting that Midjourney, DALL-E, and Adobe Firefly all have built-in filters that bar the creation of pornographic content.)

“Creating these images is easier than ever,” the letter reads, “as anyone can download the AI tools to their computer and create images by simply typing in a short description of what the user wants to see. And because many of these AI tools are ‘open source,’ the tools can be run in an unrestricted and unpoliced way.”

As we have previously covered, it has also become relatively easy to create AI-generated deepfakes of people without their consent using social media photos. The attorneys general mention a similar concern, extending it to images of children:

Advertisement
“AI tools can rapidly and easily create ‘deepfakes’ by studying real photographs of abused children to generate new images showing those children in sexual positions. This involves overlaying the face of one person on the body of

another. Deepfakes can also be generated by overlaying photographs of otherwise unvictimized children on the internet with photographs of abused children to create new CSAM involving the previously unharmed children."

"Stoking the appetites of those who seek to sexualize children"

When considering regulations about AI-generated images of children, an obvious question emerges: If the images are fake, has any harm been done? To that question, the attorneys general propose an answer, stating that these technologies pose a risk to children and their families regardless of whether real children were abused or not. They fear that the availability of even unrealistic AI-generated CSAM will "support the growth of the child exploitation market by normalizing child abuse and stoking the appetites of those who seek to sexualize children."

Regulating pornography in America has traditionally been a delicate balance of preserving free speech rights but also protecting vulnerable populations from harm. Regarding children, however, the scales of regulation tip toward far stronger restrictions due to a near-universal consensus about protecting kids. As the US Department of Justice writes, "Images of child pornography are not protected under First Amendment rights, and are illegal contraband under federal law." Indeed, as the Associated Press notes, it's rare for 54 politically diverse attorneys general to agree unanimously on anything.

However, it's unclear what form of action Congress might take to prevent the creation of these kinds of images without restricting individual rights to use AI to generate legal images, an ability that may incidentally be affected by technological restrictions. Likewise, no government can undo the release of Stable Diffusion's AI models, which are already

widely used. Still, the attorneys general have a few recommendations:

Advertisement

> *First, Congress should establish an expert commission to study the means and methods of AI that can be used to exploit children specifically and to propose solutions to deter and address such exploitation. This commission would operate on an ongoing basis due to the rapidly evolving nature of this technology to ensure an up-to-date understanding of the issue. While we are aware that several governmental offices and committees have been established to evaluate AI generally, a working group devoted specifically to the protection of children from AI is necessary to ensure the vulnerable among us are not forgotten.*
>
> *Second, after considering the expert commission's recommendations, Congress should act to deter and address child exploitation, such as by expanding existing restrictions on CSAM to explicitly cover AI-generated CSAM. This will ensure prosecutors have the tools they need to protect our children.*

It's worth noting that some fictional depictions of CSAM are illegal in the United States (although it's a complex issue), which may already cover "obscene" AI-generated materials.

Establishing a proper balance between the necessity of protecting children from exploitation and not unduly hamstringing a rapidly unfolding tech field (or impinging on individual rights) may be difficult in practice, which is likely why the attorneys general recommend the creation of a commission to study any potential regulation.

In the past, some well-intentioned battles against CSAM in technology have included controversial side effects, opening doors for potential overreach that could affect the privacy and rights of law-abiding people. Additionally, even though

CSAM is a very real and abhorrent problem, the universal appeal of protecting kids has also been used as a rhetorical shield by advocates of censorship.

AI has arguably been the most controversial tech topic of 2023, and using evocative language that paints a picture of rapidly advancing, impending doom has been the style of the day. Similarly, the letter's authors use a dramatic call to action to convey the depth of their concern: "We are engaged in a race against time to protect the children of our country from the dangers of AI. Indeed, the proverbial walls of the city have already been breached. Now is the time to act."

https://arstechnica.com/?p=1965814

US broadband grant rules shut out small ISPs and municipalities, advocates say

Getty Images | Andrey Denisyuk

reader comments

23 with

The biggest Internet service providers will dominate a $42.45 billion broadband grant program unless the Biden administration changes a rule requiring grant recipients to obtain a letter of credit from a bank, according to a joint statement from consumer advocacy groups, local government

officials, and advocates for small ISPs.

The letter sent today to US government officials argues that "by establishing capital barriers too steep for all but the best-funded ISPs, the LOC [letter-of-credit requirement] shuts out the vast majority of entities the program claims to prioritize: small and community-centered ISPs, minority and women-owned ISPs, nonprofits, and municipalities."

The rule is part of the Broadband Equity Access and Deployment (BEAD) program that's being administered by the National Telecommunications and Information Administration (NTIA).

"Rather than demonstrating a provider's ability to construct a broadband network and provide high-speed broadband services to unserved and underserved Americans, the LOC is a measure of whether they can lock up valuable working capital over multiple years," the letter said. "While large incumbents may be able to bear this financial burden, most others can not. And, due to various state and local rules, municipalities are often not allowed to obtain LOCs. Therefore, alternatives to the LOC are critical to ensure these providers can participate in the BEAD program."

The director of the BEAD program, Evan Feinman, responded to letter-of-credit concerns during a webinar in June. He said the NTIA is aiming to "minimize the failure rate, because every project that's undertaken will expend some funds prior to failing and then have to start back at square one with a new provider if it turns out that a provider doesn't have the wherewithal to undertake a project."

"We know that when we narrow [who can get funding], we're going to lose the opportunity to get into partnership with some high-quality small outfits. But we had to err on one side or the other, there was no way to hit it right on the nose," Feinman said. The NTIA will waive the LOC requirement on a case-by-case basis, but waivers will be "tightly controlled,"

he said.

Advertisement

Biden’s former FCC nominee among 300 letter-signers

Today’s letter objecting to the letter-of-credit rule was signed by “a coalition of 300 broadband experts, ISPs, community leaders, nonprofits, consumer advocates, and business groups,” said the Benton Institute for Broadband & Society. Local government officials from various parts of the US were among the signers.

One signer is Gigi Sohn, the longtime consumer advocate who was nominated by President Biden to the Federal Communications Commission. After the US Senate refused to confirm her nomination, Sohn became executive director of the nonprofit American Association for Public Broadband that lobbies for municipal networks.

The letter was signed by advocates from various other broadband-focused groups, including Public Knowledge; Connect Humanity; the Schools, Health & Libraries Broadband Coalition; the Institute for Local Self-Reliance; Free Press; Next Century Cities; the Multicultural Media, Telecom, and Internet Council; the Coalition for Local Internet Choice; and Consumer Reports.

The letter was sent to Secretary of Commerce Gina Raimondo and NTIA Administrator Alan Davidson. Describing the BEAD program requirements, the letter said that participants must obtain a letter of credit “issued by an FDIC bank with Weiss rating of B- or better for 25 percent of the award amount.”

Rules strike wrong balance, letter says

Funding rules are intended to ensure that ISPs deliver on commitments to build networks. As we wrote last month, some ISPs that won grants from a different federal program are trying to escape their broadband-deployment commitments.

But the letter to the NTIA and Commerce Department argued that the letter-of-credit requirement is a bad method of ensuring compliance:

> *Banks providing LOCs require that they be collateralized by cash or cash-equivalent. As a result, awardees will have to lock away vast sums of capital for the full duration of the build, likely several years. With the additional 25 percent match requirement, recipients will have a capital hurdle of more than 60 percent of their grant. We estimate a provider seeking a $7.5 million grant for a $10 million project will need at least $4.6 million of their own capital up-front.*
>
> *While we support the NTIA's intention of ensuring providers are accountable for delivering on grants, far from safeguarding taxpayer dollars, the LOC requirement will prevent the Internet service providers best positioned to connect unserved and underserved Americans from participating.*

ISPs that signed the letter include Astound Broadband (owner of Grande, RCN, and Wave) and several smaller providers. A lobby group for small providers, the Wireless Internet Service Providers Association, signed as well.

https://arstechnica.com/?p=1965846

YouTube under no obligation to host anti-vaccine advocate’s videos, court says

reader comments

80 with

A prominent anti-vaccine activist, Joseph Mercola, yesterday lost a lawsuit attempting to force YouTube to provide access to videos that were removed from the platform after YouTube banned his channels.

Mercola had tried to argue that YouTube owed him more than $75,000 in damages for breaching its own user contract and denying him access to his videos. However, in an order dismissing Mercola’s complaint, US magistrate judge Laurel Beeler wrote that according to the contract Mercola signed, YouTube was “under no obligation to host” Mercola’s content after terminating his channel in 2021 “for violating YouTube’s Community Guidelines by posting medical misinformation about COVID-19 and vaccines.”

“The court found no breach because ‘there is no provision in the Terms of Service that requires YouTube to maintain particular content’ or be a ‘storage site for users’ content,'” Beeler wrote.

Because Mercola’s contract with YouTube was found to be

enforceable and “YouTube had the discretion to take down content that harmed its users,” Beeler said that Mercola did not plausibly plead claims for breach of contract or unjust enrichment.

Mercola’s complaint was dismissed without leave to amend.

Ars could not immediately reach Google or Mercola for comment.

Mercola’s losing arguments against YouTube

In his complaint, Mercola described himself as “a board-certified physician and leader in the field of natural health” who “was an early user of YouTube and began sharing video content in or around 2005, the year YouTube was founded.”

Over time, Mercola amassed 300,000 subscribers to a YouTube channel that “garnered 50 million views” by boosting professionally made videos that linked to his website, “which promotes natural health and provides health articles, optimal wellness products, medical news, and a free newsletter.”

Researchers and regulators described Mercola’s background to The New York Times a little differently. They claimed that he was at one point the “most influential spreader of coronavirus misinformation” and profited “from misleading claims about Covid-19 vaccines.”

Advertisement
But Mercola said that YouTube never sent him any notices that his content was out of line with the video platform’s community guidelines. He also claimed that after YouTube updated its policy to prevent COVID-19 misinformation, he “carefully avoided posting any content that mentioned Covid-19 vaccines or discussed the Covid-19 outbreak in a manner that YouTube might determine was out of line with official government positions on Covid-19.”

Mercola claimed that he first became aware that YouTube was planning to ban his channel when The Washington Post published an article about it. He told the Post that he was being censored. In his complaint, he said that within six minutes of the Post's article publishing, he got a message that his channels were banned, effective immediately, for violating YouTube's new policy on vaccine misinformation.

His attempt to appeal YouTube's decision was denied, according to Beeler's order. At that point, YouTube told Mercola that after reviewing his channel "carefully," YouTube "confirmed that it violates our Community Guidelines."

"We won't be putting your channel back up on YouTube," the email said.

With no other option to fight back, Mercola sued, alleging that YouTube had failed to provide "advance notice of the vaccine-misinformation policy before terminating the channel and account," warn Mercola of the termination or act fairly and in good faith. He also claimed that YouTube failed to give him access to his content, which he claimed that YouTube's terms of use required. Finally, he said that YouTube had been unjustly enriched for retaining his content and converting it exclusively to YouTube's use.

Beeler rejected all these arguments, agreeing with YouTube that there was no breach of contract, no damages should be awarded, and Section 230 of the Communications Decency Act barred Mercola's claims.

"YouTube had the discretion to terminate channels without warning after a single case of severe abuse," Beeler wrote. "Under the contract, this determination was discretionary: the contract said that '[i]f we reasonably believe that any Content is in breach of this agreement or may cause harm… we may remove or take down that Content in our discretion.'"

Commenting on Mercola's case, legal expert Eric Goldman wrote:

“Lawsuits over content removals never succeed.”

https://arstechnica.com/?p=1965538

Sony copyright claims for Bewitched spell trouble for group that preserves old TV [Updated]

Enlarge / Everyday witch Samantha Stephens and the rest of the *Bewitched* crew.

reader comments

81 with

[Update at 6:56 pm ET: It looks like Rick Klein will be able to keep the YouTube channel running. Sony’s copyright office emailed Klein after this article was published, saying it would “inform MarkScan to request retractions for the notices issued in response to the 27 full-length episode postings of *Bewitched*” in exchange for “assurances from you that you or the Fuzzy Memories TV Channel will not post or re-post any infringing versions from *Bewitched* or other content owned or distributed by SPE [Sony Pictures Entertainment] companies.”

Sony said it’s taking that step because “this is the first time we have become aware of your YouTube Channel posting unauthorized versions of SPE-distributed content, and the

unique circumstances therein." However, Sony told Klein that his channel must remove "similarly infringing posts for other SPE-distributed shows," pointing out that he had posted episodes from other Sony shows.]

Original story: A nonprofit that preserves classic television videos may have its YouTube channel shut down tomorrow over copyright claims for *Bewitched* episodes that originally aired in the 1960s.

The Museum of Classic Chicago Television has about 5,000 videos, including many decades-old commercials and news shows, posted on its YouTube channel and its own Fuzzy Memories website. President and chief curator Rick Klein's "quest to save vintage Chicago TV shows and commercials" was featured in a WBEZ story two years ago.

But after 16 years of Klein and his group, who rely on donors and volunteers, archiving old videos, the TV museum's YouTube channel on August 30 received six copyright strikes for posting 27 *Bewitched* episodes owned by Sony Pictures Television. Copyright complaints were sent by MarkScan, a "digital asset protection" firm that content owners hire to enforce copyrights. MarkScan has been sending copyright complaints on Sony's behalf since at least 2014.

Advertisement

Klein told Ars today that he's not opposed to the *Bewitched* videos' deletion and that he has no intention of reposting them. But over the past few days he has been trying to reach anyone at MarkScan or Sony who can reverse the copyright strikes so he can continue the Museum of Classic Chicago Television's YouTube channel.

"We have received copyright strikes before, and the majority of the time were able to resolve them outside of the YouTube system—just by, you know, two humans talking to each other," Klein told us in an email. "It's hard to have a conversation

with a faceless corporate behemoth, though.”

YouTube owner Google provides copyright holders the option of scheduling a removal request to take effect in seven days, which gives the uploader a week to delete the content and avoid a copyright strike. Klein wishes MarkScan had used that less punitive option. “We would have just immediately deleted the videos and that would have been the end of it,” he said. “But they decided to go right to takedowns with immediate strikes, and without even emailing us ahead of time to simply ask if we would remove the videos—which we would have.”

“Arbitrary” copyright strikes

Klein’s predicament was reported yesterday by TorrentFreak, which noted that MarkScan’s copyright enforcement on behalf of Sony is sometimes a bit sloppy. MarkScan last year sent a copyright complaint to Google about Sony content posted on an India-based streaming service that is owned by Sony itself.

Copyright strikes are issued to YouTube page operators when a copyright owner has “submitted a complete and valid legal takedown request for using their copyright-protected content,” according to a support page on YouTube copyright strikes. Three strikes within a short time period makes a YouTube channel “subject to termination.”

Advertisement
Copyright strikes expire after 90 days, but that doesn’t help Klein because he received six in one day. The other options provided by YouTube owner Google are to “get in touch with the person who claimed your video and ask them to retract their claim of copyright infringement” or submit a counter-notification arguing that “your video was removed by mistake, or qualifies as fair use.”

The notification from YouTube to Klein, which he shared with Ars, shows that the channel got five strikes containing five

Bewitched videos each and a sixth strike containing two *Bewitched* videos. Klein said the 27 *Bewitched* videos were all "from broadcasts and specialty 16mm network prints." They were all removed automatically as part of the copyright claim process.

"To say this is arbitrary is blatantly obvious," Klein told Ars. "The videos were all of the same 'offending' material… why not just issue one strike for the whole batch? Those videos would still be removed, so MarkScan/Sony would still get what they want. What is the purpose of issuing multiple strikes if not to be cruelly and senselessly punitive?"

Klein said he contacted MarkScan by sending "multiple emails at multiple times from multiple accounts, and to multiple email addresses that we were able to find—all to no avail." He also sent an email to Sony's copyright email address.

"We have no issues deleting the material and never uploading it again—that was never the complaint, nor are we asking for more rights to display material than the copyright holder is willing to grant—we're just asking that if a company doesn't want something uploaded to let us know first or give us a chance to remove it voluntarily before destroying 16+ years of effort and tens of thousands of hours of work," he told us.

https://arstechnica.com/?p=1965506

Reddit faces content quality concerns after its Great Mod

Purge

Aurich Lawson

reader comments

186 with

Did you know that improper food canning can lead to death? Botulism—the result of bacteria growing inside improperly treated canned goods—is rare, but people can die from it. In any case, they'll certainly get very ill.

The dangers of food canning were explained to me clearly, succinctly, and with cited sources by Brad Barclay and someone going by Dromio05 on Reddit (who asked to withhold their real name for privacy reasons). Both were recently moderators on the r/canning subreddit and hold science-related master's degrees.

Yet Reddit removed both moderators from their positions this summer because Reddit said they violated its Moderator Code of Conduct. Mods had refused to end r/canning's protest against Reddit and its new API fees; the protest had made the entire subreddit "read only." Now, the ousted mods fear that r/canning could become subject to unsafe advice that goes unnoticed by new moderators. "My biggest fear with all this is that someone will follow an unsafe recipe posted on the sub and get badly sick or killed by it," Dromio05 told me.

Reddit's infamous API changes have ushered in a new era for the site, and there are still questions about what this next chapter will look like. Ars Technica spoke with several former mods that Reddit booted—and one who was recently appointed by Reddit—about concerns that relying on replacement mods with

limited subject matter expertise could result in the spread of dangerous misinformation.

Questions about replacement mods' expertise

When Reddit announced it would abruptly start charging significant fees for access to its API, many third-party Reddit apps announced they would close (and many have). Some Reddit users, including mods, also quit Reddit. In addition, Reddit revoked the mod badges from long-time moderators and subsequently sought replacements, though some expelled mods worry that the replacements weren't carefully selected or trained.

Advertisement
Barclay told me he moderated r/canning for three years before Reddit nuked his badge. He noted various canning misconceptions, from thinking the contents of a concave lid are safe to eat to believing you don't need to apply heat to food in jars.

He claimed that some new r/canning moderators appointed by Reddit had previously shown a lack of canning expertise before getting the new volunteer gig. For example, Barclay pointed to one mod recommending "citizen science," saying they would use a temperature data logger to "begin conducting experiments to determine what new canning products are safe." Reddit later made that user an r/canning mod.

Dromio05 showed me several posts he deemed questionable since Reddit took away his own mod badge. For example, this post shares a link to an article about "rebel canners," which Dromio05 argues "gives a public platform to people who openly encourage methods and recipes that are known to be unsafe, like canning milk and open kettle canning." The post is labeled unsafe, but Dromio05 would have removed the link to

the article.

Another cited example is this recipe for canned sauce. It includes already-canned tomatoes, which experts like the National Center for Home Food Preservation (NCHFP) recommend against, as there’s no safe tested process for this. The recipe also includes nuts, though the USDA doesn’t have any recommendations for canning nuts, and NCHFP and other experts advise against canning any nuts besides green peanuts.

The new mod team for r/canning declined to comment on this story.

There are many schools of thought around any broad topic such as canning, of course, and the former canning mods I spoke with had slightly different standards for whether or not a post could be considered safe enough for the subreddit. What’s critical for Reddit’s content quality is not that moderators adopt identical philosophies but that they are equipped to facilitate healthy and safe discussions and debates that benefit the community.

Newly implemented replacement mods represent a fraction of the over 50,000 moderators Reddit says it has. But the hastiness with which these specific replacement mods were ushered in, and the disposal of respected, long-time moderators, raises questions about whether Reddit prioritized reopening subreddits to get things back to normal instead of finding the best people for the volunteer jobs.

https://arstechnica.com/?p=1961446

Apple details reasons to abandon CSAM-scanning tool, more controversy ensues

reader comments

111 with

In December, Apple said that it was killing an effort to design a privacy-preserving iCloud photo scanning tool for detecting child sexual abuse material (CSAM) on the platform. Originally announced in August 2021, the project had been controversial since its inception. Apple first paused it that September in response to concerns from digital rights groups and researchers that such a tool would inevitably be abused and exploited to compromise the privacy and security of all iCloud users. This week, a new child safety group known as Heat Initiative told Apple that it is organizing a campaign to demand that the company "detect, report, and remove" child sexual abuse material from iCloud and offer more tools for users to report CSAM to the company.

Today, in a rare move, Apple responded to Heat Initiative, outlining its reasons for abandoning the development of its iCloud CSAM scanning feature and instead focusing on a set of on-device tools and resources for users known collectively as "Communication Safety" features. The company's response to Heat Initiative, which Apple shared with WIRED this morning, offers a rare look not just at its rationale for pivoting to

Communication Safety, but at its broader views on creating mechanisms to circumvent user privacy protections, such as encryption, to monitor data. This stance is relevant to the encryption debate more broadly, especially as countries like the United Kingdom weigh passing laws that would require tech companies to be able to access user data to comply with law enforcement requests.

Advertisement

“Child sexual abuse material is abhorrent and we are committed to breaking the chain of coercion and influence that makes children susceptible to it,” Erik Neuenschwander, Apple’s director of user privacy and child safety, wrote in the company’s response to Heat Initiative. He added, though, that after collaborating with an array of privacy and security researchers, digital rights groups, and child safety advocates, the company concluded that it could not proceed with development of a CSAM-scanning mechanism, even one built specifically to preserve privacy.

“Scanning every user’s privately stored iCloud data would create new threat vectors for data thieves to find and exploit,” Neuenschwander wrote. “It would also inject the potential for a slippery slope of unintended consequences. Scanning for one type of content, for instance, opens the door for bulk surveillance and could create a desire to search other encrypted messaging systems across content types.”

WIRED could not immediately reach Heat Initiative for comment about Apple’s response. The group is led by Sarah Gardner, former vice president of external affairs for the nonprofit Thorn, which works to use new technologies to combat child exploitation online and sex trafficking. In 2021, Thorn lauded Apple’s plan to develop an iCloud CSAM scanning feature. Gardner said in an email to CEO Tim Cook on Wednesday, which Apple also shared with WIRED, that Heat Initiative found Apple’s decision to kill the feature “disappointing.”

“We firmly believe that the solution you unveiled not only positioned Apple as a global leader in user privacy but also promised to eradicate millions of child sexual abuse images and videos from iCloud,” Gardner wrote to Cook. “I am a part of a developing initiative involving concerned child safety experts and advocates who intend to engage with you and your company, Apple, on your continued delay in implementing critical technology … Child sexual abuse is a difficult issue that no one wants to talk about, which is why it gets silenced and left behind. We are here to make sure that doesn’t happen.”

Advertisement

Apple maintains that, ultimately, even its own well-intentioned design could not be adequately safeguarded in practice, and that on-device nudity detections for features like Messages, FaceTime, AirDrop, the Photo picker are a safer alternatives. Apple has also begun offering an application programming interface (API) for its Communication Safety features so third-party developers can incorporate them into their apps. Apple says that the communication platform Discord is integrating the features and that app makers broadly have been enthusiastic about adopting them.

“We decided to not proceed with the proposal for a hybrid client-server approach to CSAM detection for iCloud Photos from a few years ago,” Neuenschwander wrote to Heat Initiative. “We concluded it was not practically possible to implement without ultimately imperiling the security and privacy of our users.”

On Heat Initiative’s request that Apple create a CSAM reporting mechanism for users, the company told WIRED that its focus is on connecting its vulnerable or victimized users directly with local resources and law enforcement in their region that can assist them rather than Apple positioning itself as a middle man for processing reports. The company says that offering this intermediary service may make sense

for interactive platforms like social networks.

The need to protect children from online sexual abuse is urgent, though, and as these concerns intersect with the broader encryption debate, Apple’s resolve on refusing to implement data scanning will continue to be tested.

Read the full exchange between Heat Initiative and Apple at WIRED. WIRED has redacted sensitive personal information for the privacy of senders and recipients.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1964978