Damning probes find Instagram is key link connecting pedophile rings

reader comments

51 with

Instagram has emerged as the most important platform for buyers and sellers of underage sex content, according to investigations from The Wall Street Journal, Stanford Internet Observatory, and the University of Massachusetts Amherst (UMass) Rescue Lab.

While other platforms play a role in processing payments and delivering content, Instagram is where hundreds of thousands—and perhaps millions—of users search explicit hashtags to uncover illegal "menus" of content that can then be commissioned. Content on offer includes disturbing imagery of children self-harming, "incest toddlers," and minors performing sex acts with animals, as well as opportunities for buyers to arrange illicit meetups with children, the Journal reported.

Because the child sexual abuse material (CSAM) itself is not hosted on Instagram, platform-owner Meta has a harder time detecting and removing these users. Researchers found that even when Meta's trust and safety team does ban users, their efforts are "directly undercut" by Instagram's recommendation system—which allows the networks to quickly reassemble under "backup" accounts that are usually listed in the bios of original accounts for just that purpose of surviving bans.

A Meta spokesperson told Ars that the company works “aggressively to fight” child exploitation on all its platforms “and to support law enforcement in its efforts to arrest and prosecute the criminals behind it.” Because criminals’ tactics “constantly change,” Meta said it has enacted “strict policies and technology to prevent them from finding or interacting with teens on our apps” and hired “specialist teams who focus on understanding their evolving behaviors so we can eliminate abusive networks.” These efforts led Meta to dismantle 27 abusive networks between 2020 and 2022 and ban 490,000 accounts violating child safety policies in January 2023, the spokesperson reported.

But these tactics do not appear to be doing enough to combat the problem, researchers said. UMass Rescue Lab director Brian Levine told Ars that it took his team minutes to uncover pedophile rings operating on Instagram after identifying “simple tags” used to help connect buyers and sellers. The Wall Street Journal reported that the hashtags researchers identified could be obvious, like “pedowhore,” or rely on code words, like “cheese pizza,” which shares initials to allude to child pornography.

Advertisement

Levine said that since Instagram’s trust and safety team has broader access to search the platform, it should be able to monitor for hashtags more effectively than outside researchers. However, the team does not seem to be effectively monitoring the situation, as it’s missing easily discoverable hashtags.

This was the first time Levine’s lab looked into Instagram as part of the team’s work to research online child victimization and build tools to prevent it, Levine told Ars.

“I think their trust and safety team needs a lot of help,” Levine added.

In research published yesterday investigating self-generated CSAM (SG-CSAM) allegedly posted by minors advertising their own content, Alex Stamos, Stanford Internet Observatory (SIO) director, told Ars that his team didn't specifically target Instagram. But the team found that the platform's recommendation system "plays a particularly important role as the discovery mechanism that introduces buyers to sellers." Levine told Ars that Instagram has an obligation to ensure its recommendation system does not promote abusive content.

The Journal revealed that Instagram repeatedly failed to ban hashtags, take down content, and prevent promotion once content was detected. After the Journal sent inquiries, for example, Meta confirmed that it was "in the process of removing" hashtags promoting illegal materials like "pedobait" or "mnsfw" (minor not safe for work) and admitted that it "permitted users to search for terms that its own algorithms know may be associated with illegal material." A Meta spokesperson told Ars that it has already "restricted thousands of additional search terms and hashtags on Instagram."

The WSJ reported that Instagram was so ineffective at stopping pedophile rings from forming that it would sometimes display a pop-up screen when users searched for known abusive content, warning users that "these results may contain images of child sexual abuse." Users could then choose to "see results anyway" or "get resources" regarding the harms of consumption of abusive content. Meta told the Journal that it was removing this option but failed to explain why the option was ever given in the first place.

Meta also admitted that it has repeatedly failed to act on reports of child abuse on Instagram because of "a software glitch" preventing reports from ever being processed. This bug has reportedly since been fixed. Now Meta said it will provide additional training for content reviewers and assemble an internal task force "to investigate these claims and

immediately address them.”

https://arstechnica.com/?p=1946320

Pornhub attacks states for passing “unsafe” age-verification laws

Getty Images | Pornhub

reader comments

36 with

Starting today, Pornhub visitors in Virginia, Mississippi, and Arkansas will see a “very important message” on the adult website’s homepage. Pornhub’s public service announcement prompts visitors to contact representatives and oppose recently passed age-verification laws in these states that Pornhub claims puts children and all users’ privacy at risk. If users don’t support Pornhub before laws go into effect, the company says, Pornhub could potentially restrict access in these states—a threat it already followed through on in Utah.

In the PSA, adult entertainer Cherie Deville tells Pornhub users that instead of states requiring ID to access adult content, “the best and most effective solution for protecting children and adults alike is to verify users’ age at a device level and allow or block access to age-restricted materials and websites accordingly.”

According to CNN, this PSA is part of a larger effort by Pornhub and its private equity owners, Ethical Capital Partners (ECP), to work with big tech companies to create new device-based age verification solutions. So far, ECP partner Solomon Friedman told CNN that ECP has lobbied Apple, Google, and Microsoft to "develop a technological standard that might turn a user's electronic device into the proof of age necessary to access restricted online content."

ECP, Apple, Google, and Microsoft did not immediately respond to Ars' request for comment.

Pornhub is not commenting beyond the PSA, but a spokesperson told Ars that Pornhub supports age verification laws that don't put user safety and privacy at risk.

Advertisement
Currently, Pornhub is complying with a Louisiana law requiring an ID to access the site, but Pornhub's spokesperson said Pornhub was one of the few adult entertainment sites to do so. As a result of complying, Pornhub's Louisiana traffic dropped by approximately 80 percent as adult content seekers presumably chose to visit sites that do not require ID. This makes the Internet more unsafe, Pornhub argues, by shuffling users away from sites with safety measures in place to dark corners of the web.

"As we've seen in other states where similar laws have passed, this just drives activities to other sites with far fewer or even no safety measures in place," Deville said. "This clearly demonstrates that poorly executed age verification solutions only make the Internet more unsafe."

Pornhub reported that Louisiana users have already experienced identity theft as a result of the age verification law there. That's a big part of why Pornhub sees device-based age verification as a preferred solution, compared to submitting IDs or requiring facial scans—which forces all compliant adult

sites to collect sensitive data that could be leaked and harm users.

“Giving your ID card every time you want to visit an adult platform is not the most effective solution for age verification,” Deville warned. “In fact, it will put children and your privacy at risk.”

While Friedman told CNN that ECP’s talks with tech companies to create more effective device-based solutions are only in “early stages,” Deville suggested that acceptable device-based solutions already exist and could be leveraged.

“Many devices already offer free and easy-to-use parental control features that can prevent kids from accessing adult content without risking the disclosure of your sensitive data,” Deville said.

But critics told CNN that there’s one obvious flaw of device-based age verification: Minors could simply access adult content by using an adult’s device, especially since families and households frequently share devices.

https://arstechnica.com/?p=1946132

Inside 4chan’s top-secret moderation machine

Anjali Nair/Getty Images

reader comments

53 with

On May 14, 2022, 18-year-old Payton Gendron sent out a link to a select group of online friends. It was an invite to a private Twitch stream, access to his running online diary, and an upload of his 180-page manifesto.

Those who clicked the link saw Gendron sitting in his car, in the parking lot of the Tops supermarket in Buffalo, New York. They watched as he lifted his AR-15-style rifle, equipped with a high-capacity magazine, and opened fire. He killed 10 people in just six minutes.

Even before police stopped the massacre and arrested Gendron, the link was being posted to the anonymous imageboard 4chan. On /pol/, the site's "politically incorrect" board, people commented in real time on the mass shooting. "Why not shoot up the abortion rallys? What a faggot," one user wrote. Another chimed in: "The kids manifesto is actually pretty good." Dozens of people who missed the livestream demanded a recording. Others declared it a deep-state false flag operation.

One poster, however, was imploring the site's users to accept responsibility. "Why is this place so full of hate and anger?" they asked. "It's like a den of inequity [sic]. Why don't you people ever express love or compassion?" They uploaded a photo of Payton Gendron, and named the file "the 4chan killer."

"You made Payton Gentron [sic], a sociopathic mass murderer," they wrote.

4chan's moderators soon jumped in and banned the user's account, deleting their comment. The reason for the ban:

“Complaining about 4chan.”

Advertisement

The way in which 4chan is managed and moderated is of growing interest among US government officials. The US House of Representatives’ January 6 committee subpoenaed 4chan over its role in facilitating the assault on the US Capitol, while investigators with the New York Attorney General’s Office ordered the company to turn over thousands of records to better understand its role in Gendron’s terrorist attack. WIRED obtained a number of internal 4chan documents through a public records request.

Those documents show how 4chan’s team of moderators—janitors, in their own nomenclature—manage the site. Internal emails, chat logs, and moderation decisions reveal how the site’s janitors have helped shape it in their own image, using their moderation powers to engender 4chan’s particular brand of edgelord white supremacy. In particular, the documents show how the site’s moderators responded to a wave of attention as their website had, once more, been cited as an ideological driver for an act of mass murder.

More than that, the documents lay bare the degree to which 4chan’s toxic influence is a design, not a bug.

In his manifesto, Gendron credited 4chan with showing him “the truth”—that is, a deeply paranoid and racist belief that “the White race is dying out.” He selected the Tops supermarket specifically because it was in a predominantly Black neighborhood. 4chan, too, told him what to do about it. Years earlier, browsing the site, he had come across a video of 28-year-old Brenton Tarrant stalking through the Al Noor mosque in Christchurch, New Zealand, in 2019, murdering 51 people.

In launching the attack in Buffalo, Gendron was following in Tarrant’s footsteps. He even liberally plagiarized Tarrant’s manifesto. And he made regular use of 4chan’s insular, hateful

lexicon of memes and in-jokes.

While Gendron has pled guilty to murder, domestic terrorism, and hate crimes charges, and is awaiting trial on additional federal charges, the families of some of the victims have filed a lawsuit against a number of social media companies, including 4chan, Discord, Reddit, Snapchat, Alphabet, Meta, and Amazon. They allege that Gendron's radicalization was caused by an inability, or outright refusal, by these companies to stem the flow of violent conspiracy theories online.

https://arstechnica.com/?p=1945646

SEC sues Binance, says it evaded US law with "extensive web of deception"

Enlarge / Binance founder and CEO Changpeng Zhao speaks virtually during the Web3 Blockchain Festival in Hong Kong, China, on Wednesday, April 12, 2023.
Getty Images | Bloomberg

reader comments

124 with

The US Securities and Exchange Commission today sued Binance and its CEO/founder Changpeng Zhao, alleging that the defendants' "blatant disregard" of federal law "enriched

themselves by billions of US dollars while placing investors' assets at significant risk."

"Defendants have unlawfully solicited US investors to buy, sell, and trade crypto asset securities through unregistered trading platforms available online at Binance.com and Binance.US," alleged the SEC complaint in US District Court for the District of Columbia.

Binance's CCO (chief compliance officer) "bluntly admitted to another Binance compliance officer in December 2018, 'we are operating as a fking unlicensed securities exchange in the USA bro,'" according to the lawsuit. The CCO was also quoted as saying, "We do not want [Binance].com to be regulated ever."

The SEC is seeking fines, disgorgement of ill-gotten gains with interest, and injunctions. In a press release, the SEC alleged that "while Zhao and Binance publicly claimed that US customers were restricted from transacting on Binance.com, Zhao and Binance in reality subverted their own controls to secretly allow high-value US customers to continue trading on the Binance.com platform."

SEC Chair Gary Gensler said that Binance entities and Zhao "engaged in an extensive web of deception, conflicts of interest, lack of disclosure, and calculated evasion of the law." They "actively conceal[ed] who was operating the platform… and even where and with whom investor funds and crypto assets were custodied" and "attempted to evade US securities laws by announcing sham controls that they disregarded behind the scenes so that they could keep high-value US customers on their platforms," he said.

Advertisement

Binance accuses SEC of overreach

Defendants also include related companies BAM Trading Services

and BAM Management US Holdings Inc. The SEC lawsuit has 13 charges alleging violations of the Securities Act and Exchange Act. The complaint is similar to one filed in March against Binance and Zhao by the US Commodity Futures Trading Commission (CFTC). As we previously wrote, the CFTC lawsuit seeks disgorgement, civil monetary penalties, and permanent trading and registration bans.

Binance issued a response to the SEC on Monday. It said there is "zero justification" for the lawsuit, that the SEC is trying "to claim jurisdictional ground from other regulators," and that "any allegations that user assets on the Binance.US platform have ever been at risk are simply wrong."

"All user assets on Binance and Binance affiliate platforms, including Binance.US, are safe and secure, and we will vigorously defend against any allegations to the contrary," Binance said. Binance further accused the SEC of "overreach" and said that "because Binance is not a US exchange, the SEC's actions are limited in reach."

Binance is the world's largest crypto asset trading platform, with a trading volume of $9.58 trillion in 2021, the SEC lawsuit said. Binance is said to have earned at least $11.6 billion in revenue from June 2018 to July 2021, mostly from transaction fees.

Binance's own cryptocoin offering, BNB, was down over 10 percent in trading following today's SEC lawsuit.

SEC: Binance chose to evade US law

The lawsuit alleged that under Zhao's control, Binance and affiliated entities "have unlawfully offered three essential securities market functions—exchange, broker-dealer, and clearing agency—on the Binance Platforms without registering with the SEC. Acutely aware that US law requires registration for these functions, Defendants nevertheless chose not to

register, so they could evade the critical regulatory oversight designed to protect investors and markets."

Advertisement

Binance claimed to the public that Binance.com didn't serve US people "while simultaneously concealing their efforts to ensure that the most valuable US customers continued trading on the platform," the SEC said, continuing:

> *When the Binance.US Platform launched in 2019, Binance announced that it was implementing controls to block US customers from the Binance.com Platform. In reality, Binance did the opposite. Zhao directed Binance to assist certain high-value US customers in circumventing those controls and to do so surreptitiously because—as Zhao himself acknowledged—Binance did not want to "be held accountable" for these actions. As the Binance CCO explained, "[o]n the surface we cannot be seen to have US users[,] but in reality, we should get them through other creative means." Indeed, Zhao's stated "goal" was "to reduce the losses to ourselves, and at the same time to make the US regulatory authorities not trouble us."*

The SEC said that Zhao and Binance tried to evade US regulatory oversight by creating BAM Management and BAM Trading in the US and by "claim[ing] publicly that these entities independently controlled the operation of the Binance.US Platform." But Zhao and Binance controlled things behind the scenes and "Zhao continues to own 81 percent of BAM Management," the SEC said. "Neither BAM Management nor any of its subsidiaries or affiliated entities (including BAM Trading) has ever been registered with the SEC in any capacity."

In November 2020, "BAM Trading's then-CEO told Binance's CFO that her 'entire team feels like [it had] been duped into being a puppet,'" according to the SEC lawsuit.

Besides the requested monetary penalties and disgorgement, the SEC is seeking a jury trial and injunctions requiring “asset freezes, a verified accounting, repatriation of assets, expedited discovery, preservation of documents and information, prohibition on the destruction of evidence, the appointment of a receiver, alternative service, and/or any other necessary equitable relief that the Court deems just and proper.”

https://arstechnica.com/?p=1945525

YouTube now allows videos that falsely claim Trump won 2020 election

Enlarge / A Trump campaign event in Waco, Texas, on Saturday, March 25, 2023.
Getty Images | Bloomberg

reader comments

280 with

YouTube on Friday announced a major change in its approach to US election misinformation, saying it will no longer remove videos that make false claims about the 2020 election or previous presidential elections. Starting today, “we will stop removing content that advances false claims that widespread fraud, errors, or glitches occurred in the 2020 and other past

US Presidential elections," YouTube's announcement said.

This is a reversal from YouTube's announcement in December 2020 that it would ban videos falsely claiming that Donald Trump beat Joe Biden. YouTube said at the time that it "will start removing any piece of content uploaded today (or anytime after) that misleads people by alleging that widespread fraud or errors changed the outcome of the 2020 US Presidential election, in line with our approach towards historical US Presidential elections. For example, we will remove videos claiming that a Presidential candidate won the election due to widespread software glitches or counting errors."

The Google subsidiary YouTube made its December 2020 announcement while Trump was spreading a baseless conspiracy theory that the election was stolen from him. Trump's false claims helped fuel the January 6, 2021, attack on the US Capitol.

YouTube today said it "carefully deliberated" before deciding to drop the policy:

> *We first instituted a provision of our* ***elections misinformation policy*** *focused on the integrity of past US Presidential elections in December 2020, once the states' safe harbor date for certification had passed. Two years, tens of thousands of video removals, and one election cycle later, we recognized it was time to reevaluate the effects of this policy in today's changed landscape. In the current environment, we find that while removing this content does curb some misinformation, it could also have the unintended effect of curtailing political speech without meaningfully reducing the risk of violence or other real-world harm.*

YouTube's policy against false claims still applies to certain elections in other countries, specifically the 2021 German federal election, and the Brazilian presidential elections in 2014, 2018, and 2022.

Advertisement

YouTube reversed Trump ban in March

YouTube said other policies that reduce spread of misinformation about US elections will not be changed. The platform said it will continue to "disallow content aiming to mislead voters about the time, place, means, or eligibility requirements for voting; false claims that could materially discourage voting, including those disputing the validity of voting by mail; and content that encourages others to interfere with democratic processes."

YouTube also said it will continue to promote "authoritative" content about elections. "We are ensuring that when people come to YouTube looking for news and information about elections, they see content from authoritative sources prominently in search and recommendations," YouTube said.

Like other social networks, YouTube suspended Trump's account after the US Capitol attack. YouTube allowed Trump back on in March of this year, saying, "We carefully evaluated the continued risk of real-world violence, while balancing the chance for voters to hear equally from major national candidates in the run up to an election. This channel will continue to be subject to our policies, just like any other channel on YouTube."

Twitter reversed its ban on Trump in November 2022, shortly after Elon Musk bought the company. Meta announced it would allow Trump back on Facebook in January 2023.

https://arstechnica.com/?p=1944197

Twitter safety chief resigns after Musk criticizes decision to restrict film

Getty Images | NurPhoto

reader comments

398 with

Twitter VP of Product Trust and Safety Ella Irwin resigned from the company yesterday, she confirmed to Reuters and other news outlets. Irwin's departure came on the same day that Twitter owner Elon Musk criticized his staff for restricting *What Is a Woman?*, a controversial Daily Wire documentary on transgender issues that has been labeled as transphobic by many.

Irwin took over as head of Twitter's trust and safety team after the November 2022 resignation of Yoel Roth. Twitter has massively reduced its staff under Musk's leadership and is facing scrutiny from regulators, particularly in the European Union, over its content moderation practices. Twitter executive A.J. Brown, the head of brand safety and ad quality, also left this week.

Twitter recently pulled out of the EU's voluntary Code of Practice on Disinformation but must comply with the mandatory Digital Services Act rules taking effect on August 25. As European Commissioner for Internal Market Thierry Breton tweeted, "obligations remain. You can run but you can't hide. Beyond voluntary commitments, fighting disinformation will be [a] legal obligation under DSA as of August 25. Our teams will

be ready for enforcement."

Irwin "declined to comment on the reason for her departure in an interview with The Wall Street Journal," the newspaper reported. "She said she felt she had always been honest in her work. Irwin, who joined Twitter about a year ago, had publicly defended the company's actions since Musk took over as she navigated a high-profile and often-scrutinized role handling content-moderation decisions."

Advertisement
Roth explained his resignation in November. He stayed at Twitter for a short time after Musk took over but said, "One of my limits was if Twitter starts being ruled by dictatorial edict rather than by policy… there's no longer a need for me in my role, doing what I do." Roth also criticized Musk's "rapid-fire layoffs and an ill-fated foray into reinventing Twitter's verification system."

Internal dissent over misgendering

Irwin's resignation seems to have been precipitated by internal dissent over how to enforce Twitter's Hateful Conduct policy, which was recently edited to remove a ban on "targeted misgendering or deadnaming of transgender individuals." The policy still bans direct attacks on people on the basis of gender or gender identity; the dehumanization of a group of people based on gender or gender identity; and hateful imagery that promotes hostility and malice against people based on gender identity.

Daily Wire co-founder and co-CEO Jeremy Boreing wrote yesterday morning that "Twitter canceled a deal with the Daily Wire to premiere *What is a Woman?* for free on the platform because of two instances of 'misgendering.'"

"Twitter let us know that not only could we no longer purchase the package they offered, they would no longer provide us any

support and would actually limit the reach of the film and label it as ‘hateful conduct’ because of ‘misgendering,'” he wrote. “Specifically: In the film, a father refers to his 14-year-old daughter as ‘her,’ and a store owner uses the ‘wrong’ pronoun in a confrontation with a trans person.”

Boreing said the Daily Wire reminded Twitter that misgendering was removed from its hateful conduct policy. According to Boreing, Twitter then “clarified they only removed ‘misgendering’ from their policy because they didn’t need to be that specific, but that they still consider ‘misgendering’ abuse and harassment.” Twitter further told the Daily Wire “that our own followers would not be able to see [the movie] in their feeds,” he wrote.

https://arstechnica.com/?p=1944048

No groundwater, no new homes, as Arizona severely restricts new housing

Enlarge / Aerial view of a subdivision in the Phoenix suburb of Scottsdale.

reader comments

261 with

The nation’s fifth-largest city and surrounding metropolitan area is officially tapped out of groundwater, Arizona Gov.

Katie Hobbs announced Thursday, adding another item to the state's long list of water woes.

By 2121, the Phoenix metro area will be short of nearly 5 million acre feet of water—enough water for around 17 million homes—under a new groundwater model released Thursday by the Arizona Department of Water Resources.

That means any new development in the region that hasn't had its water guaranteed will have to rely on another source of water, such as the Colorado River and other local rivers, or on yet-to-be developed sources like desalinated ocean water, recycled wastewater, or groundwater pumped from other basins in the state, to ensure existing homes and developments have the water they need in the future.

Advertisement

Since 1957, Arizona's population has surged 555 percent, while water usage has decreased 3 percent. Much of the state's growth has come in the form of sprawling suburbs built on cheap land in the desert, which often relies solely on groundwater.

Sarah Porter, the director of Arizona State University's Kyl Center for Water Policy, said Thursday's announcement means developers will now have to weigh the cost of building on more expensive land that has an assured water supply, or find new water sources on land that can no longer rely on groundwater, as climate change produces intensifying droughts.

State officials cautioned the model shows the state's groundwater laws are working and that Arizona's water supply is secure and would only largely impact certain areas in the region.

When Arizona passed its Groundwater Management Act in 1980, the state decided it would keep track of groundwater in the most populated parts of the state, Porter said. With the modeling showing the Phoenix metro area is not adequately

replenishing the groundwater it is taking out of its aquifer, the state is stopping growth on that finite resource.

“The regulations are working to prevent homes from being sold and then having no water,” Porter said.

https://arstechnica.com/?p=1943967

Pentagon buying Starlink dishes for Ukraine after funding dispute with SpaceX

Enlarge / Starlink satellite dish seen on September 25, 2022 in Izyum, Kharkiv region, amid the Russian invasion of Ukraine.
Getty Images | Yasuyoshi Chiba

reader comments

96 with

The US Defense Department confirmed today that it is buying Starlink satellite broadband service for use in Ukraine.

“We continue to work with a range of global partners to ensure Ukraine has the satellite and communication capabilities they need. Satellite communications constitute a vital layer in Ukraine’s overall communications network and the department contracts with Starlink for services of this type,” the Defense Department said in a statement provided to Ars and

other media outlets today.

The Pentagon said it would not provide other details about contracts, capabilities, or partners because of "operational security reasons and due to the critical nature of these systems." According to a Bloomberg report, the deal includes Starlink satellite terminals and services to be used by the Ukraine military.

Deal seems to resolve funding dispute

In September, SpaceX asked the Pentagon to fund the Ukraine government and military's use of Starlink, saying it couldn't afford to donate more user terminals or pay for operations indefinitely. SpaceX CEO Elon Musk backtracked on October 15, writing, "The hell with it… even though Starlink is still losing money & other companies are getting billions of taxpayer $, we'll just keep funding Ukraine govt for free."

At the time, SpaceX withdrew its funding request, but the Pentagon and SpaceX held talks about funding Starlink in Ukraine. Musk wrote in an October 2022 tweet that "25,300 terminals were sent to Ukraine, but, at present, only 10,630 are paying for service."

Advertisement

It's not clear when the current deal was struck. As Bloomberg's article today notes, the Defense Department said in December that it would provide Ukraine with satellite communications terminals and services but didn't confirm a contract with SpaceX at that time. Bloomberg wrote:

> *The terminals will likely be purchased under the Ukraine Security Assistance Initiative, which provides for the embattled nation's long-term security needs. In December, the Defense Department disclosed in announcing such a funding*

> *package that it would provide satellite communications "terminals and services" to Ukraine, but didn't confirm that Musk's company would get the contract.*

Also in December, Ukraine government official Mykhailo Fedorov said that Ukraine would get 10,000 more Starlink terminals in the ensuing months thanks to a new deal with SpaceX and funding from several European countries.

SpaceX objected to "offensive" use by Ukraine

Although SpaceX provided Starlink terminals to Ukraine shortly after the Russian invasion early last year, the company objected to its service being "weaponized" by the Ukraine military. As a result, SpaceX confirmed that it took steps to prevent Ukraine's military from using Starlink satellite Internet with drones.

SpaceX knows "the military is using them for comms, and that's OK," President and COO Gwynne Shotwell reportedly said in February. "But our intent was never to have them use it for offensive purposes."

An Economist report in March said that "Starlink now uses geofencing to block the use of its terminals—not only above Russian-occupied territory inside Ukraine, but also, according to a Ukrainian military intelligence source, over water and when the receiver is moving at speeds above 100km per hour."

Musk wrote in a February tweet that "Starlink is the communication backbone of Ukraine, especially at the front lines, where almost all other Internet connectivity has been destroyed. But we will not enable escalation of conflict that may lead to WW3."

https://arstechnica.com/?p=1943740

FTC: Amazon/Ring workers illegally spied on users of home security cameras

Enlarge / Amazon Ring indoor cameras displayed during an event at company headquarters in Seattle on September 25, 2019.
Getty Images | Bloomberg

reader comments

83 with

A Federal Trade Commission lawsuit filed yesterday accused Ring, the home security camera company owned by Amazon, of invading users' privacy by "allowing thousands of employees and contractors to watch video recordings of customers' private spaces."

Until September 2017, every employee of Ring and a Ukraine-based contractor had access to customer videos, which were stored without encryption, the FTC said. "Ring gave every employee—as well as hundreds of Ukraine-based third-party contractors—full access to every customer video, regardless of whether the employee or contractor actually needed that access to perform his or her job function," the FTC said.

Violations did not stop in 2017 despite new access controls, according to the lawsuit, which alleges privacy invasions both before and after Amazon bought Ring in 2018. The FTC's lawsuit in US District Court for the District of Columbia also alleged

that Ring failed to promptly implement basic privacy and security protections, making it easier for hackers to take over customers' accounts and cameras. A settlement that is pending a judge's approval would require Ring to pay $5.8 million for customer refunds, delete certain types of data, and implement privacy and security controls. Amazon did not admit any wrongdoing.

In a press release, the FTC said that "Ring deceived its customers by failing to restrict employees' and contractors' access to its customers' videos, using customer videos to train algorithms, among other purposes, without consent, and failing to implement security safeguards." In one case, an employee "viewed thousands of video recordings belonging to female users of Ring cameras that surveilled intimate spaces in their homes such as their bathrooms or bedrooms," the FTC said.

That allegedly occurred between June and August 2017 and invaded the privacy of at least 81 female users of Ring products. "The employee wasn't stopped until another employee discovered the misconduct. Even after Ring imposed restrictions on who could access customers' videos, the company wasn't able to determine how many other employees inappropriately accessed private videos because Ring failed to implement basic measures to monitor and detect employees' video access," the FTC said.

Advertisement

In a separate action announced yesterday, the FTC and US Department of Justice charged Amazon with violating the Children's Online Privacy Protection Act (COPPA) "by keeping kids' Alexa voice recordings forever and undermining parents' deletion requests." A pending settlement would force Amazon to pay a $25 million fine; delete children's data, geolocation data, and other voice recordings; and take other steps to improve privacy.

Amazon reported net sales of $127.4 billion and net income of $3.2 billion in the first quarter.

FTC calls Ring security too sloppy

The FTC complaint against Ring alleged that it failed to implement multifactor authentication and other protections against credential-stuffing and brute-force attacks until 2019 and that the implementation of security measures was too sloppy. Ring made two-factor authentication available in May 2019 "but did not take reasonable steps to encourage its adoption, such as through user-friendly opt-ins for existing customers and default opt-outs for new users," the complaint said. Fewer than 2 percent of Ring customers adopted the optional security feature in 2019.

The FTC complaint said:

> *During the course of these attacks, approximately 55,000 US customers suffered serious account compromises. For at least 910 US accounts (affecting approximately 1,250 devices), the bad actor not only accessed the accounts, but took additional invasive actions, such as accessing a stored video, accessing a live stream video, or viewing a customer's profile. The bad actors disproportionately targeted indoor cameras… in many instances, the bad actors were not just passively viewing customers' sensitive video data. Rather, the bad actors took advantage of the camera's two-way communication functionality to harass, threaten, and insult individuals—including elderly individuals and children—whose rooms were monitored by Ring cameras, and to set off alarms and change important device settings.*

Ring also "implemented some forms of rate limiting before July 2019," but the rate limiting didn't cover all authentication portals and "failed to block multiple attempts in rapid succession to log into different accounts from the same IP

address," the FTC said. The 55,000 credential-stuffing and brute-force attacks cited by the FTC allegedly occurred between January 2019 and March 2020.

https://arstechnica.com/?p=1943611

It's prison day for Elizabeth Holmes; 11-year sentence has begun in Texas

Enlarge / Elizabeth Holmes, founder of Theranos Inc., center, arrives at Federal Prison Camp Bryan in Bryan, Texas, US, on Tuesday, May 30, 2023.

reader comments

219 with

Disgraced biotech entrepreneur Elizabeth Holmes has arrived at a federal prison in Texas to begin her 11-year, three-month sentence for defrauding investors of her defunct blood-testing startup, Theranos.

Press and photographers stationed outside the women's prison camp in Bryan, Texas, captured what appeared to be Holmes exiting a gray SUV with New York state plates and making her way into the facility flanked by facility staff at around 12:30 pm local time. Shortly afterward, the Federal Bureau of Prisons confirmed to the Associated Press that Holmes was indeed in custody at the facility, FPC Bryan, which is about

100 miles northwest of Houston.

The facility houses about 655 female inmates who are required to work in the cafeteria or a manufacturing facility, with pay starting at $1.15 per hour, according to The New York Times. Like other inmates, Holmes will don prison-issued khaki pants and shirts in pastel green, gray, or white during her stay. She will have no Internet access but can buy a radio or an MP3 player from the prison commissary and listen to “non-explicit” music. When she’s not working or listening to prison-approved music, she can partake in leisure activities such as “table games” and arts and crafts.

Advertisement

In January 2022, Holmes was convicted on four counts of defrauding Theranos investors for falsely claiming that her propriety blood-testing device could run hundreds of tests with just a small drop of blood. In truth, the device never actually worked. Last November, the judge in her case, US District Judge Edward Davila, sentenced her to 11 years and three months in prison—a hefty term meant to send a message to Silicon Valley about the dangers of hubris and the “fake it till you make it” ethos.

Holmes is appealing her conviction, but the prospects of overturning it appear dim. She also requested to remain free on bail during the appeal process, a request denied by both Davila and a three-judge panel for the US Court of Appeals for the 9th Circuit, where she is appealing her conviction. On May 17, Davila ordered Holmes to report to prison today, May 30, no later than 2 pm.

Davila also ordered Holmes, along with her ex-boyfriend and former Theranos President, Ramesh “Sunny” Balwani, to pay $452 million in restitution to defrauded investors. The two, who were tried separately, are jointly responsible for paying back the sum. Balwani, who was convicted on 12 counts of defrauding investors, patients, and doctors, has already begun his nearly 13-year prison sentence.

Reporting to prison today, Holmes leaves behind two small children and their father, her new partner, Billy Evans. The couple reportedly have a boy, William, born in July 2021 and a three-month old daughter named Invicta, which is Latin for “invincible.”

Holmes’ children can visit their mother in person on weekends and federal holidays. Holmes is allowed to hold them in her lap. They are also allowed phone and video calls, but calls are limited to 15 minutes each with a total of 300 minutes per month.

The Times notes that three women escaped FPC Bryan in 2017, one of whom has not been found.

https://arstechnica.com/?p=1942984