Meta has no choice but to sell Giphy at $262M loss to Shutterstock

reader comments

43 with

Talk about a fire sale. With limited interest in GIF platforms and UK regulators forcing a sale, Meta has decided to sell Giphy to Shutterstock for a mere $53 million. After purchasing it for $315 million in 2020 and subsequently being ordered to sell it by the UK's Competition and Markets Authority (CMA), Meta has been challenged to find a suitable Giphy buyer at a time when GIFs are perceived to be less trendy than three years ago. The GIF library has found a fitting future owner in Shutterstock, but for Meta, it means a $262 million loss.

The deal

Shutterstock announced today its definitive agreement to buy Giphy for $53 million, seven months after Meta said it would accept the CMA's ruling that it must divest Giphy. Shutterstock said the deal is expected to close in June and is "subject to customary closing conditions."

The deal should assuage trepidation from Giphy, which encouraged the CMA to enact behavioral ordinances rather than force Meta to sell Giphy. The animated images company feared GIFs just weren't as cool as they were in 2020, and so the platform would mostly attract "weak or inappropriate" suitors.

"User sentiment towards GIFs on social media shows that they

have fallen out of fashion as a content form, with younger users in particular describing GIFs as ‘for boomers’ and ‘cringe,’” Giphy told the CMA in August.

Giphy urged the CMA, which had to approve Meta’s Giphy sale, to wait for a buyer with “industry knowledge and experience managing a group of young tech engineers, product managers, and staff.”

Advertisement

Shutterstock gettin’ Giphy wit it

It’s unclear how “young” Shutterstock’s team is, but Giphy’s library will at least be an appropriate inclusion in the stock image provider’s library. Meanwhile, Shutterstock hopes to expand more into consumers.

Shutterstock plans to incease its API ecosystem with Giphy’s 14,000-plus API/SDK integrations. It will gain 1.7 billion daily users implementing more than 1.3 billion searches daily and generating 15 billion daily media impressions, including across the Giphy website and app, today’s announcement claimed.

The New York City-headquartered company will also add new partners, since Giphy is integrated with business platforms like Microsoft Teams and Slack and social media ones like TikTok and SnapChat. Meta has also signed a deal to continue leveraging Giphy’s API.

Further, Giphy has partnered with media entities, including Disney, NBC, and Netflix, and sports leagues, like the NFL. Shutterstock hopes to use these to grow its marketing and advertising potential by getting consumers to use relevant GIFs and stickers in “casual conversations,” Shutterstock CEO Paul Hennessy said in a statement.

“We plan to leverage Shutterstock’s unique capabilities in

content and metadata monetization, generative AI, studio production and creative automation to enable the commercialization of our GIF library as we roll this offering out to customers," he said.

According to CNBC, Shutterstock shares rose almost 2 percent during Tuesday's morning trading.

https://arstechnica.com/?p=1941299

Facebook hit with record €1.2 billion GDPR fine for transferring EU data to US

Getty Images | SOPA Images

reader comments

65 with

European and Irish regulators have ordered Facebook owner Meta to pay a fine of 1.2 billion euros for violating the General Data Protection Regulation (GDPR) with transfers of personal data to the United States. It's the largest GDPR fine ever.

Meta was also ordered to stop storing European Union user data in the US within six months, but it may ultimately not have to take that step if the EU and US agree on a new regulatory framework for international data transfers.

The infringement by Meta's subsidiary in Ireland "is very serious since it concerns transfers that are systematic, repetitive, and continuous," European Data Protection Board (EDPB) Chair Andrea Jelinek said in an announcement today. "Facebook has millions of users in Europe, so the volume of personal data transferred is massive. The unprecedented fine is a strong signal to organizations that serious infringements have far-reaching consequences."

The Ireland Data Protection Commission (DPC) decided not to fine Meta in July 2022, but the ruling was subject to binding dispute resolution after some regulators in other European countries objected. The EDPB then overruled Ireland's DPC and instructed it to amend the draft to impose a fine.

The EDPB also said it instructed Ireland regulators to order Meta "to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of European users transferred in violation of the GDPR, within six months after notification" of the final decision.

Meta and a tech-industry trade group criticized the ruling. The Computer & Communications Industry Association (CCIA), which represents Meta and other tech companies, said the order to suspend data transfers "effectively makes the way the Internet works illegal, from video conferencing and browsing the Internet, to the processing of online payments."

Advertisement

While the Ireland DPC's draft decision in July 2022 didn't include a fine, it said that Facebook's data transfers should be suspended. The DPC's view was that "exercise of additional corrective powers, beyond the proposed suspension order, would exceed the extent of powers that could be described as being 'appropriate, proportionate and necessary' to address the infringement of Article 46(1) GDPR," the Irish regulator said.

“Highest degree of negligence”

Meta was found to violate article 46(1) of the GDPR, which says companies may only transfer personal data to another country if there are “appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.”

The EDPB’s binding decision said that Meta “committed the infringement of Article 46(1) with at least the highest degree of negligence” and that the infringement affects “a wide range of categories of personal data.” Meta’s design of Facebook “prevents it from providing this service” in Europe without the international data transfers that were found to violate the GDPR, “which suggests that a considerable part of its profits derived from the provision of the service in the EU arise from the breach of the GDPR,” the EDPB said.

A fine is necessary because of “the gravity of the infringement, taking into account the particularly large scope of the processing and the very high number of data subjects affected, as well as the long duration of the infringement, which is still ongoing,” the EDPB decision said. The Ireland DPC issued a final decision that incorporates the required changes.

In a blog post, Meta executives said the company is “appealing these decisions and will immediately seek a stay with the courts who can pause the implementation deadlines, given the harm that these orders would cause, including to the millions of people who use Facebook every day.”

Meta hopes EU/US pact will come soon

Meta also said that “there is a fundamental conflict of law between the US government’s rules on access to data and

European privacy rights.”

EU and US officials have been negotiating a deal on data transfers. Meta said that if the pending EU-US Data Privacy Framework “comes into effect before the implementation deadlines expire, our services can continue as they do today without any disruption or impact on users.”

“This decision is flawed, unjustified, and sets a dangerous precedent for the countless other companies transferring data between the EU and US,” Meta wrote.

https://arstechnica.com/?p=1940912

China bans Micron’s products from key infrastructure, citing security risk

reader comments

107 with

China said US chipmaker Micron Technology’s products posed “serious network security risks” as it banned operators of key infrastructure from buying them, in its first big measure against an American semiconductor group.

The Cyberspace Administration of China on Sunday announced that the company, which is the biggest US maker of memory

chips, “posed significant security risks to China’s critical information infrastructure supply chain.” As a result, it ordered “critical national infrastructure operators” to stop purchasing products from Idaho-based Micron.

The move follows a seven-week investigation into Micron by the CAC, a probe that was widely seen as retaliation for US efforts to curb China’s access to critical technology. Last October, Washington introduced expansive chip export controls, and the Netherlands and Japan have since followed.

The US Department of Commerce said it strongly opposed the action, which it said had “no basis in fact.”

“This action, along with recent raids and targeting of other American firms, is inconsistent with the PRC’s assertions that it is opening its markets and is committed to a transparent regulatory framework,” the Department of Commerce said.

It said it would engage with Chinese authorities to seek clarification. “We also will engage with key allies and partners to ensure we are closely coordinated to address distortions of the memory chip market caused by China’s actions,” it added.

Analysts said Micron presented an obvious first target for Beijing as its tech would be more easily replaced with competitors’ chips from South Korean rivals Samsung and SK Hynix. Last month the White House asked South Korea to urge its chipmakers not to fill any market gap in China if the sale of Micron products was restricted.

Advertisement

China is an important market for Micron. Mainland China and Hong Kong generated 25 percent of its $30.8 billion in revenue last year, according to a person familiar with the matter.

Paul Triolo, an expert on China tech at consultancy Albright Stonebridge, said: “This could be really bad for Micron. It

depends how broad China’s definition of critical information infrastructure is, but this could include the financial sector, transportation, energy and data centers.”

He added that data centers were a particularly important customer for Micron memory chips.

Beijing’s edict comes a day after G7 leaders issued a stark rebuke of China during the annual meeting of global leaders in Hiroshima, decrying its human rights record, “non-market” economic policies, and increasing military assertiveness in the East and South China Seas.

Micron chief executive Sanjay Mehrotra was part of a delegation of business leaders who attended the G7 summit. He dined with US Ambassador to Japan Rahm Emanuel and Citi chief Jane Fraser on Saturday night in the Japanese coastal town.

“We have received the CAC’s notice of conclusion of its review of Micron products sold in China,” Micron said in a statement. “We are evaluating the conclusion and assessing our next steps. We look forward to continuing to engage in discussions with Chinese authorities.”

China informed Micron of its decision in a meeting in Beijing on Sunday, according to a person familiar with the matter. Micron had received no communication from CAC after responding to questions from the regulator in March until it was summoned for a meeting this weekend, the person said.

“This is new for China,” Triolo said of the Micron ban, adding that Beijing was not taking the US actions “lying down.”

In its statement, the CAC said that “China welcomes global companies and various platform products into the China market as long as they follow China’s laws and regulations.” The regulator’s statement did not provide any information on the “security risks” posed by Micron’s products.

Analysts warned that Beijing’s restrictions could even prompt Chinese companies that did not provide “critical information infrastructure” to seek to eliminate Micron from their supply chains.

“The blast radius could be much bigger,” said Triolo.

© 2023 The Financial Times Ltd. All rights reserved. Not to be redistributed, copied, or modified in any way.

https://arstechnica.com/?p=1940872

France is fighting to save your iPhone from an early death

Enlarge / An iPhone undergoes repairs.

reader comments

53 with

Every time a new iPhone comes out, a team of technicians in the French city of Toulouse start to pull it apart. In the three years they’ve been doing this, they’ve found a device that’s gradually transforming into a fortress. Today’s iPhones are packed with parts that cannot be repaired or replaced by anyone other than an expensive Apple-accredited repair shop. And France doesn’t like that one bit.

It’s a problem that’s been getting worse and worse, says Alexandre Isaac, CEO of The Repair Academy, the renowned research and training group that runs the Toulouse workshop. Every time a new iPhone is released, his team finds another part that’s been locked to work only with a specific Apple device. First it was just a chip on the motherboard, he says. Then the list of parts with repair restrictions stretched to Touch ID, Face ID, and eventually the battery, the screen, and the camera.

By forcing people to pay an accredited technician more than the value of a second-hand iPhone for a simple repair job, Apple is incentivizing people to throw their devices away rather than fix them, says Isaac. The Repair Academy estimates an Apple-accredited technician charges customers twice as much as an independent repair shop. “A lot of people see Apple as super green,” Isaac says, referring to the solar panels on the company’s California headquarters and the recycled aluminum used to build MacBooks. The Repair Academy has been gathering evidence to try and prove that’s not the case. Instead, Apple’s engineers are proactively trying to make iPhones harder to repair, he argues.

Advertisement

It’s a problem Isaac has been following for years. And now a Paris prosecutor has decided to take action. On May 15, the prosecutor announced that there will be an official investigation into allegations that Apple is pursuing a business model of planned obsolescence—a term that refers to designing a product in a way that intentionally limits its lifespan.

The prosecutor, which has delegated the investigation to France’s Department of Competition, Consumer Affairs, and Fraud Prevention (DGCCRF), will have powers to fine the

company and also prove whether Apple’s iPhone repair restrictions break French law, as campaigners claim. For years, France has been at the forefront of the right to repair movement, introducing Europe’s first repairability scoring system. But this case cements the country’s willingness to take on Apple and the way it builds its products.

“France is pushing for the right to repair in ways that nobody else has yet,” says Elizabeth Chamberlain, sustainability director at iFixit, a US group that campaigns for the right to repair. “This is the first time we’ve seen any movement against planned obsolescence via parts-pairing at a national level.” Apple did not reply to WIRED’s request for comment. The company recently published its 2023 environmental progress report.

https://arstechnica.com/?p=1940745

AT&T tries to block Starlink/T-Mobile plan for satellite-to-phone service

Enlarge / A flag on the fifth green during the first round of the AT&T Byron Nelson golf tournament at TPC Craig Ranch on May 11, 2023, in McKinney, Texas.
Getty Images | Mike Mulholland

reader comments

47 with

AT&T and other entities are trying to block the SpaceX/T-Mobile plan to provide Starlink satellite service directly to cell phones.

In a filing yesterday, AT&T urged the Federal Communications Commission to reject the SpaceX/T-Mobile proposal. “The FCC’s rules do not permit SpaceX’s proposed use of T-Mobile’s terrestrial spectrum, and Applicants fail to even request—much less justify—rule waivers that would be necessary to authorize their proposed SCS [supplemental coverage from space] authorizations,” AT&T said.

AT&T said it is interested in the proceeding because it has a license to use adjacent spectrum in the PCS C Block. AT&T says the SpaceX/T-Mobile plan, which was announced in August 2022, could “jeopardize or inhibit the delivery of terrestrial wireless services,” including mobile broadband.

SpaceX and T-Mobile’s “technical showings are woefully insufficient regarding the risk of harmful interference posed by their planned SCS deployments,” AT&T told the FCC. “SpaceX and T-Mobile’s applications fall far short of meeting the threshold for waiver and cannot be granted in their current state.”

Plan affects up to 7,500 satellites

The FCC last month sought comment on the application, noting that SpaceX requested modification of its license for low-orbit Earth satellites “to add a direct-to-cellular communications capability on up to 7,500 Gen2 Starlink satellites.” The links to consumer devices would rely on the 1910-1915 MHz (Earth-to-space) and 1990-1995 MHz (space-to-Earth) bands, also known as PCS G-Block, the FCC said.

The FCC is on board with satellite companies and mobile carriers partnering to close gaps in wireless networks. In a March action, the FCC proposed a new regulatory framework to

help satellite operators and wireless companies “leverage the growth in space-based services to connect smartphone users in remote, unserved, and underserved areas.” But the FCC could still reject or require changes to the SpaceX/T-Mobile plan.

Advertisement
We contacted SpaceX and T-Mobile today and will update this article if we get any response.

SpaceX said recently that it plans to start testing the satellite-to-cell system with T-Mobile sometime this year. Text messaging is expected to be the first supported service, with voice and Internet coverage to be added later.

Rural wireless group has similar objections

The SpaceX/T-Mobile docket also drew responses yesterday from the Rural Wireless Association, a trade group for small, rural wireless carriers, and Omnispace, which is partnering with Ligado for a satellite-to-phone system.

The RWA told the FCC it is concerned “that T-Mobile’s and SpaceX’s proposed operations may cause adjacent channel interference to licensees’ mobile and fixed network operations in the 1895-1910 MHz and 1975-1990 MHz bands (‘PCS C-Block’) in rural and remote areas.”

SpaceX told the FCC that its “direct-to-cellular system will operate without causing harmful interference to or requiring protection from any other service duly licensed in these bands” and “will protect adjacent band operations from harmful interference.”

But according to the RWA, “SpaceX offers no support for this conclusion nor does it offer to put any protections in place to ensure there is no adjacent channel interference.” SpaceX and T-Mobile also have not “provided the results of any field

trials that would allow the public to analyze the potential for adjacent channel interference," the rural wireless group said. Omnispace similarly told the FCC that the SpaceX/T-Mobile plan would interfere with existing mobile-satellite service networks.

One other opposition filing came in two weeks ago from the National Radio Astronomy Observatory, a government-funded research center. The group said the SpaceX/T-Mobile plan would cause harmful interference in portions of the National Radio Quiet Zone. SpaceX issued a response saying that the astronomy group's concerns "appear more appropriately addressed in the Commission's general rulemaking to establish industry-wide rules for SCS."

The FCC sided with SpaceX in a separate battle over spectrum use yesterday. As we reported, the FCC rejected a Dish Network proposal for mobile service in the 12.2-12.7 GHz band, saying the Dish plan would cause harmful interference to satellite broadband service.

https://arstechnica.com/?p=1940732

Twitter claims Microsoft broke API rules; Musk already threatened lawsuit

Getty Images | Christopher Furlong

reader comments

203 with

Elon Musk’s lawyer, Alex Spiro, yesterday sent a letter to Microsoft accusing the company of using the Twitter APIs in ways that violated Twitter policies. Spiro’s letter came about a month after Microsoft halted API use instead of paying new fees and Musk threatened to sue Microsoft, claiming it was “illegally using Twitter data.”

“As you are no doubt aware, for years, Microsoft has used Twitter’s standard developer APIs free of charge in order to benefit from Twitter’s data and services in key Microsoft products that generate tens of billions of dollars in revenue for Microsoft annually,” Spiro wrote to Microsoft CEO Satya Nadella. “Up until last month, when it declined to pay even a discounted rate for continued access to Twitter’s APIs and content, Microsoft operated eight separate Twitter API apps, listed below, which appear to provide data and functionality for at least five separate Microsoft products and services, including Xbox One, Bing Pages, Azure, Power Platform, and Ads.”

Twitter—which is facing numerous lawsuits alleging it hasn’t paid its bills—is asking Microsoft to complete a compliance audit on its API usage by June 7.

Spiro’s letter said that by registering to use the Twitter API, Microsoft agreed to comply with Twitter’s rules. “However, our recent review of Microsoft’s activity on the Microsoft Apps indicates that Microsoft may have been in violation of multiple provisions of the Agreement for an extended period of time,” Spiro wrote.

Microsoft accused of exceeding rate limits

One of Spiro's allegations is that Microsoft exceeded Twitter's API rate limits. Spiro did not cite a specific limit but said that Twitter prohibits API users from exceeding or circumventing the API limits and prohibits use of the Twitter API "in a manner that exceeds reasonable request volume" or "constitutes excessive or abusive usage."

"Microsoft Apps accessed Twitter's APIs over 780 million times and retrieved over 26 billion tweets in 2022 alone," he wrote. "Indeed, for one of the Microsoft Apps, Microsoft's account information outright states that it intends to allow its customers to 'go around throttling limits.'"

When contacted by Ars, Microsoft provided a statement confirming it received the letter. "We heard from a law firm representing Twitter with some questions about our previous use of the free Twitter API. We will review these questions and respond appropriately. We look forward to continuing our long term partnership with the company."

Advertisement

Spiro also alleged that Microsoft "appears to have used the Twitter API for unauthorized uses and purposes." Microsoft's "Azure Logic Apps for Fairfax app supplied Twitter content to a number of Microsoft endpoints that reference a government entity or agency, despite the fact that the Agreement prohibits use of the Twitter APIs on behalf of 'any government-related entity' without first 'identify[ing] all such Government End Users' to Twitter," the letter said.

Microsoft was required "to disclose and obtain approval for its intended use case for each Microsoft App" and notify Twitter of any substantial change to those use cases, he wrote. But the company allegedly "did not identify any use

case for six of the eight Microsoft Apps that it continued to operate until last month."

"The Agreement also prohibits the registration of multiple apps for 'a single use case or substantially similar or overlapping use cases.' But Microsoft registered multiple apps each for its Bing Pages, Ads, and Azure products and services, in clear violation of this provision," Spiro wrote.

Audit could be prelude to lawsuit

Finally, Spiro claims that Microsoft violated Twitter rules on automation when using the API for Power Platform and Ads. "Microsoft's API requests for these apps include Twitter actions that are subject to certain restrictions on automation, including retweets and direct messages," he wrote.

The letter's audit request asked for extensive details on how Microsoft used Twitter APIs over the past two years, including "identification of any and all government-related entities served by each Microsoft App." The audit request also seeks a description of how Microsoft used token pooling and "any other means implemented in the Microsoft Apps to circumvent Twitter's rate limits for the Twitter APIs."

Twitter wants the audit to identify "all Twitter Content… currently in Microsoft's possession or control," and provide records describing all Twitter content "retained by Microsoft through its use of the Twitter APIs, the manner and format in which such Twitter Content was stored, and the manner in which such Twitter Content was used by Microsoft." The Musk-owned company wants details on any Twitter content that Microsoft previously obtained and destroyed and "a description of how such Twitter Content was destroyed."

The demand for a compliance audit could be a prelude to a lawsuit. "They trained illegally using Twitter data. Lawsuit time," Musk tweeted on April 19 in a response to Microsoft

dropping Twitter from its advertising platform instead of paying Twitter’s new API fees.

https://arstechnica.com/?p=1940562

TikTokers immediately sue to block Montana’s “unconstitutional” ban

reader comments

184 with

Surprising no one, immediately after Montana became the first state to ban TikTok on Wednesday, five TikTokers in the state with thousands of followers banded together and sued to block the ban. The TikTokers argued that the ban is a huge overstep by the state because it’s “unconstitutional and preempted by federal law.”

According to their complaint, Montana’s claimed interests in enacting the ban to shield minors and prevent foreign spying “are not legitimate and do not support a blanket ban on TikTok. Montana has no authority to enact laws advancing what it believes should be the United States’ foreign policy or its national security interests, nor may Montana ban an entire forum for communication based on its perceptions that some speech shared through that forum, though protected by the

First Amendment, is dangerous."

Citing First Amendment concerns, the TikTokers argued that the ban is "substantially overbroad" and "suppresses far more speech than it may permissibly regulate." They say that restricting access to content for all users just to address concerns that minors may access some TikTok content that's "dangerous" goes too far. The First Amendment requires the government to find the "least restrictive means" of regulating speech when the government does have a "compelling" interest. Quite the opposite, Montana's ban, they argued, is an example of the government finding "the most restrictive means imaginable."

Advertisement

They also argued that the ban was designed by Montana lawmakers with the intent to substitute Montana's "view of how best to regulate the alleged national security issues arising from TikTok's United States operations for that of the United States." Not only is the responsibility of setting foreign policy "traditionally and exclusively within the federal government's power," their complaint said, but also the federal government is actively pursuing its own solutions to possibly permit TikTok to operate in the US. If such an agreement is reached with TikTok and the US, Montana's ban could end up being even more "at odds" with federal policy.

Filed in a US district court in Montana, the lawsuit targeted State Attorney General Austin Knudsen, who supported the ban and is charged with enforcing it.

A spokesperson for Knudsen, Emily Flower, told Reuters that Montana expected the lawsuit and is "fully prepared" to defend the ban.

Ars could not immediately reach TikTok, TikTokers' lawyers, or Knudsen for comment.

Yesterday, TikTok spokesperson Brooke Oberwetter told Ars that

TikTok plans to fight Montana's ban, too.

"Governor Gianforte has signed a bill that infringes on the First Amendment rights of the people of Montana by unlawfully banning TikTok, a platform that empowers hundreds of thousands of people across the state," Oberwetter said in the statement. "We want to reassure Montanans that they can continue using TikTok to express themselves, earn a living, and find community as we continue working to defend the rights of our users inside and outside of Montana."

https://arstechnica.com/?p=1940545

FCC rejects Dish 5G plan that could have made Starlink broadband "unusable"

Enlarge / A Starlink satellite dish.
Getty Images | AntaresNS

reader comments

48 with

The Federal Communications Commission sided with Starlink in a battle against Dish Network today, rejecting a Dish proposal that could have degraded Internet service for Starlink satellite users. In a 4-0 vote, the FCC decided not to authorize high-powered terrestrial mobile service in the 12.2-12.7 GHz band that is already used by Starlink customer

terminals for downloads.

The vote “ensure[s] the present and future of satellite services in the 12.2-12.7 GHz band. We recognize that millions of people rely on services in this band—and we want to see that continue,” FCC Chair Jessica Rosenworcel said at today’s meeting. The band is also used for satellite TV.

In its announcement of the vote, the FCC said it “declin[ed] to authorize two-way, high-powered terrestrial mobile use due to a significant risk of harmful interference to existing and emergent services, particularly in the growing satellite broadband market.”

Dish already uses spectrum from the 12.2-12.7 GHz band for satellite TV and wants to use the band for cellular service as well. While the FCC rejected the mobile proposal, it said it would investigate the potential to expand terrestrial fixed use or permit unlicensed use in that spectrum.

Specifically, the FCC will seek comment on allowing point-to-point fixed links in 12.2-12.7 GHz at higher power levels than the current rules allow and on “adding indoor-only underlay and unlicensed use.” The agency also teed up a plan that could eventually allow mobile broadband in the adjacent 12.7-13.25 GHz band.

Advertisement

Starlink urged users to fight Dish plan

Starlink asked users for help in its battle against Dish in June 2022, urging them to contact the FCC. “Dish has been attempting to claim new rights to the 12 GHz band, which is the spectrum you currently use to download content with Starlink,” the SpaceX subsidiary told customers at the time. “Despite technical studies dating back as far as 2016 that

refute the basis of their claims, Dish has employed paid lobbyists who are attempting to mislead the FCC with faulty analysis in hopes of obscuring the truth." The company claimed Dish's plan would make "Starlink unusable for most Americans."

"Thank you to the 100K+ Starlink customers who spoke up, the FCC voted to protect high-speed satellite Internet users from harmful interference," Starlink wrote on Twitter today. Starlink broadband has already been getting slower as more people use the network, though performance could improve as new second-generation satellites are launched by SpaceX.

FCC Commissioner Geoffrey Starks, a Democrat, said he "would have welcomed a path forward that allowed both services to thrive" in 12.2-12.7 GHz, but that the evidence shows mobile use of the band would interfere with satellite. "Based on the studies filed to date, our engineers have concluded that high-powered mobile broadband, when deployed throughout the country, will interfere with established and emerging satellite services that serve millions of consumers," Starks said.

Commissioner Nathan Simington, one of two Republicans on the FCC, said he is still "hopeful that there is a way to allow satellite and two-way high-power fixed wireless service to coexist in the 12.2 to 12.7 GHz band," but that it isn't technically feasible in the short term.

"The power levels and coverage profiles of terrestrial networks risk saturating [satellite receiver] arrays with interference from networks of powerful terrestrial transmitters, including via side lobes even when care is taken with terrestrial antenna angles," Simington said. "Barring significant technology developments driving down the price and complexity of individual array elements while driving up quality, this will probably be the case for some time to come."

https://arstechnica.com/?p=1940349

SCOTUS spares Section 230, rules Google, Twitter not liable for aiding ISIS

reader comments

67 with

Today the United States Supreme Court quashed tech industry fears that the nation's highest court might ruin the Internet by deciding that platforms should be held liable for recommending third-party content that has long been protected by Section 230 of the Communications Decency Act.

In a pair of rulings, the Supreme Court found that plaintiffs failed to state a claim when arguing that online platforms like YouTube, Twitter, and Facebook should be held liable for aiding and abetting the Islamic State of Iraq and Syria (ISIS) terrorist enterprise by recommending terrorist content ahead of attacks. As a result, both cases, *Twitter v. Taamneh* and *Gonzalez v. Google*, have been remanded to a lower court, and at least for now, the Section 230 immunity shield remains fully intact.

Supreme Court Justice Clarence Thomas delivered the opinion in the Twitter case. He concluded that allegations that Facebook,

Twitter, and YouTube knew for years that "ISIS was using their platforms but failed to stop it from doing so" were "insufficient"—even without considering Section 230 protections—to establish that the social platforms aided and abetted a specific 2017 terrorist attack on the Reina nightclub in Istanbul, Turkey. That attack, carried out for ISIS by Abdulkadir Masharipov, killed 39 victims and injured another 69.

Plaintiffs in that case argued that social platforms can be held liable for generally aiding and abetting ISIS—and profiting from "advertisements placed on ISIS' tweets, posts, and videos." But the Supreme Court found that plaintiffs fell "short" of proving their Anti-Terrorism Act (ATA) claims that platforms gave "knowing and substantial assistance" to ISIS.

"Notably, plaintiffs never allege that ISIS used defendants' platforms to plan or coordinate the Reina attack; in fact, they do not allege that Masharipov himself ever used Facebook, YouTube, or Twitter," Thomas wrote in his opinion.

Instead, plaintiffs sought to hold tech companies liable for "creating their platforms and setting up their algorithms to display content relevant to user inputs and user history," Thomas wrote, which led them to recommend terrorist content like propaganda and recruitment materials to users. Apart from blocking some ISIS content, Thomas wrote, there is "no reason" to think that "defendants selected or took any action at all with respect to ISIS' content." And allegations that "Google reviewed and approved ISIS videos on YouTube as part of a revenue-sharing system and thereby shared advertising revenue with ISIS" alleged "nothing about the amount of money that Google supposedly shared with ISIS, the number of accounts approved for revenue sharing, or the content of the videos that were approved."

Advertisement
Because platforms' algorithms "appear agnostic"—"matching any

content (including ISIS' content) with any user who is more likely to view that content"—platforms were only allegedly guilty of standing back and watching as terrorist content spread on their platforms, Thomas wrote. That's a "far cry" from proving that platforms were consciously or substantially trying to help ISIS or participate in the Reina attack, the court decided, making platforms instead appear to be passive bystanders.

"There are no allegations that defendants treated ISIS any differently from anyone else," Thomas wrote. "Rather, defendants' relationship with ISIS and its supporters appears to have been the same as their relationship with their billion-plus other users: arm's length, passive, and largely indifferent."

The ATA does not hold passive bystanders liable for terrorist activity. If it did, then email, cell phone, Internet, or any sort of communications providers—including mail delivery services—would all be liable for terrorist attacks, the court decided.

Further, finding otherwise would "necessarily hold defendants liable as having aided and abetted each and every ISIS terrorist act committed anywhere in the world," Thomas' opinion said. Partly because plaintiffs did not show that any platform "consciously and selectively chose to promote content provided by a particular terrorist group" or had some legal duty to remove ISIS content, their allegations "certainly fall short," Thomas wrote.

"There is no allegation that the platforms here do more than transmit information by billions of people, most of whom use the platforms for interactions that once took place via mail, on the phone, or in public areas," Thomas wrote. "The fact that some bad actors took advantage of these platforms is insufficient to state a claim that defendants knowingly gave substantial assistance and thereby aided and abetted those

wrongdoers’ acts.”

Because the claims raised in the other case, *Gonzalez v. Google*, depended on the Supreme Court ruling in favor of plaintiffs in *Twitter v. Taamneh*, the court ruled that *Gonzalez v. Google* also failed to state a claim under the ATA.

Attorneys for the Taamneh and Gonzalez families, Twitter, and Facebook owner Meta did not immediately respond to Ars’ request for comment.

Google’s general counsel, Halimah DeLaine Prado, told Ars that “countless companies, scholars, content creators and civil society organizations who joined with us in this case will be reassured by this result. We’ll continue our work to safeguard free expression online, combat harmful content, and support businesses and creators who benefit from the Internet.”

https://arstechnica.com/?p=1940290

Elizabeth Holmes’ no good, very bad day: Bail denied and a bill for $452 million



Enlarge / Elizabeth Holmes (C), founder and former CEO of blood-testing and life sciences company Theranos, walks with her mother Noel Holmes and partner Billy Evans into the federal courthouse for her sentencing hearing on November 18, 2022, in San Jose, California.

reader comments

163 with

Convicted fraudster Elizabeth Holmes had a rough Tuesday.

The judge in her fraud case, US District Judge Edward Davila, ordered her and her ex-boyfriend, Ramesh “Sunny” Balwani, to pay $452 million in restitution to defrauded investors of their infamous and now defunct blood-testing company, Theranos. Holmes, the company’s founder and former CEO, and Balwani, the former president, are jointly responsible for paying back the entirety of the hefty sum.

Meanwhile, a three-judge panel for the US Court of Appeals for the 9th Circuit denied Holmes’ last-ditch effort to stay out

of prison while she appeals her conviction. Last month, Holmes' challenged Davila's previous denial of bail, asking the 9th Circuit appeals court to weigh in. The move triggered an automatic delay to the start of her 11-year-and-three-month prison term while the appeals court reviewed her argument. Davila had previously ordered her to report to prison on April 27.

While her latest effort bought her a few extra weeks of freedom, the appeals court unsurprisingly denied her bail. In a one-page order Tuesday, the judges concluded that Holmes' appeal didn't raise a "substantial question" of law or fact in her case, nor would it reverse her conviction or warrant a new trial if the court sided with her. The appeal of her conviction will proceed as previously scheduled, and it was up to Davila to set a new date for Holmes to report to prison.

In filings Wednesday, Holmes requested her new prison start date be May 30, giving her time to get her affairs in order, including setting up childcare arrangements for her two young children. Davila agreed.

Balwani, who was convicted on all 12 counts of defrauding Theranos investors and patients, already began his nearly 13-year prison term last month. Balwani is also appealing his conviction and had attempted to remain out on bail during the process.

Advertisement

Rise and fall

While at the helm of Theranos, Holmes and Balwani claimed their proprietary blood testing device could accurately perform hundreds of medical tests using just a tiny drop of blood from a finger prick. Holmes became a Silicon Valley superstar, receiving glowing publicity while wooing high-stakes investors. In 2015, the company was valued at $9

billion, and Forbes listed Holmes as the richest self-made woman, with an estimated net worth of $4.5 billion.

But in 2018, federal prosecutors charged the duo with scheming to dupe investors into funding their startup technology, which never actually worked. As Davila summarized it, the government alleged that between 2010 and 2015, the two made “false statements regarding the capabilities of Theranos’s proprietary analyzer, its financial revenue streams, and device demonstrations, as well as misrepresenting Theranos’s relationships and interactions with Walgreens, the US Department of Defense, the Food and Drug Administration, pharmaceutical companies, and research institutions.”

Once the company was going, federal prosecutors allege the pair moved on to defrauding doctors and patients between 2013 and 2016. This allegedly involved “delivering marketing materials to doctors and patients regarding Theranos’s blood tests, posting misrepresentations on Theranos’s websites, and transmitting blood tests results with inaccuracies and modifications.”

In January 2022, Holmes was convicted on four counts related to defrauding investors, and Balwani was convicted last July of defrauding investors, doctors, and patients.

In Davila’s order Tuesday, he calculated that Balwani and Holmes owe restitution of $452 million. That includes paying back $397,547,268 to individual investors, including Rupert Murdoch, who invested the largest sum of $124,999,997. It also includes paying $14.5 million back to Safeway and $40 million to Walgreens, which partnered with Theranos to offer blood testing in the drugstore giant’s neighborhood stores. Davila noted that when Walgreens asked for due diligence documents about the technology, Holmes sent the pharmacy chain doctored validation documents that carried Pfizer’s logo—even though Pfizer never endorsed the Theranos’ tech and was skeptical of it and backed out of investing in the company.

It’s unclear how Balwani and Holmes will split the bill. According to court filings, Holmes only has modest assets outweighed by a $450,000 loan to pay a settlement with the Securities and Exchange Commission. She has also accrued over $30 million in legal fees.

https://arstechnica.com/?p=1939999