AT&T stock fell to 29-year low on Friday and sank another 6.7% today



Getty Images | Eugene Mymrin

reader comments

111 with

AT&T’s stock price hit a 29-year low on Friday and continued to sink today as investors fled telecom stocks on reports that cleanups of lead-covered telephone cables could cost the industry tens of billions of dollars.

AT&T stock dropped 4.1 percent to $14.50 on Friday, reportedly the lowest close since 1994. AT&T’s stock price fell another 6.7 percent to $13.53 when the market closed today.

Frontier Communications stock dropped 11.9 percent on Friday and was down 15.8 percent today. Verizon stock fell 1.8 percent on Friday and was down 7.5 percent today. Lumen (formerly CenturyLink) fell 10.2 percent Friday and was down 8.6 percent today.

Despite the notable telecom declines, the overall market continued to rise, with the S&P 500 up 0.39 percent today and the tech-focused NASDAQ up 0.93 percent.

Today's telecom losses came after the four stocks "lost a combined $18 billion in market value last week," Investor's Business Daily wrote. The losses were spurred by a Wall Street Journal investigation into lead-sheathed cables installed by phone companies across the US many decades ago.

The industry started phasing out lead in the 1950s, but the WSJ said it found evidence of more than 2,000 lead-covered cables and said there "are likely far more throughout the country."

The telecom stocks were already having a rough year. Over the past 12 months, including today's results, AT&T's stock is down 34.1 percent. Verizon is down 37.4 percent over the past year. Lumen and Frontier are down 84.2 percent and 52.8 percent during the past 12 months, respectively.

AT&T likely faces biggest total cost

Lawmakers are pressuring telcos to identify all the cables and address any potential environmental and health problems. US Sen. Edward Markey (D-Mass.) called the telecom industry's alleged lack of action "corporate irresponsibility of the worst kind."

Advertisement
New Street Research estimated that remediation could cost the

telecom industry $60 billion, according to a Telecompetitor article. AT&T has the biggest network of legacy telephone cables and could thus face the biggest cost.

“We have discussed the copper lead sheathing situation with many industry contacts and have been unable to find a reasonable way to calculate any potential liability, but believe that AT&T will have the largest exposure given its massive LEC [local exchange carrier] business as well as owning the original AT&T long haul network,” JPMorgan wrote, according to Reuters.

Wells Fargo agreed that “AT&T undoubtedly has the greatest exposure to this potential issue, as its long-distance network dates back to the late 19th century,” as quoted in a Light Reading article. Verizon, Frontier, and Lumen “likely have exposure as well of an unclear amount.”

“The fear, of course, is that addressing the lead cable issue could divert valuable capital (and resources) from projects like fiber-to-the-home and tower upgrades. It will certainly be a topic of focus around Q2 earnings, but we also don’t expect much clarity for some time,” Wells Fargo wrote.

Long-term stock impacts predicted

Investor’s Business Daily cited several other financial analysts who expect the lead-cable problem to have lasting impacts on telecom stocks. “We could see what amounts to a general telecom buyer’s strike for some time… Investors are likely to shoot first and ask questions later. After all, none of these are stocks with outsized growth stories,” MoffettNathanson analyst Craig Moffett wrote in a note to clients today.

“AT&T and Verizon likely have the greatest potential exposure in dollar terms” because of the size of their wired networks, but Lumen and Frontier don’t have large consumer wireless

businesses to soften the blow, Moffett wrote. “Frontier, by virtue of primarily being a roll-up of incumbent phone company assets, may have the greatest proportionate exposure.”

Advertisement

Goldman Sachs analyst Brett Feldman told investors that the lead-cable revelations mean it “may take the major wireline telcos longer, and cost them more, to decommission legacy networks based on copper cables that may have lead sheathing.”

The companies could face class-action lawsuits and lawsuits from attorneys general, TD Cowen analyst Gregory Williams was quoted as saying. On the other hand, the long-term financial outlook might not be as bad as feared for the companies if it turns out that the level of contamination is “overstated.”

“The range of outcomes could range from near-zero liability to billions of dollars in damages,” Williams wrote.

Telecom industry downplayed health concerns

The telco industry tried to downplay the environmental and health concerns last week. “We have not seen, nor have regulators identified, evidence that legacy lead-sheathed telecom cables are a leading cause of lead exposure or the cause of a public health issue,” the USTelecom industry trade group told Ars.

AT&T posted a response last week claiming that The Wall Street Journal’s testing was flawed. “For decades, we have managed legacy lead-clad cables in compliance with applicable laws and regulations, and we have followed industry-wide best practices to maintain this legacy infrastructure in a way that’s safe for all based on established science,” AT&T said.

USTelecom also said that lead cables don’t necessarily need to be removed. “Many considerations go into determining whether

legacy lead-sheathed telecom cables should be removed or should be left in place, including those regarding the safety of workers who must handle the cables, potential impacts on the environment, the age and composition of the cables, their geographic location, and customer needs as well as the needs of the business and infrastructure demands. The US telecommunications industry stands ready to engage constructively on this issue," the group said.

https://arstechnica.com/?p=1954536

AT&T and Verizon's ancient lead cables have US lawmakers demanding action



Enlarge / AT&T’s stand at Mobile World Congress on February 27, 2023, in Barcelona, Spain.
Getty Images | Joan Cros Garcia-Corbis

reader comments

67 with

Newly raised concerns about lead-covered telephone cables installed across the US many decades ago are putting pressure on companies like AT&T and Verizon to identify the locations of all the cables and account for any health problems potentially caused by the toxic metal.

US Sen. Edward Markey (D-Mass.) wrote a letter to the USTelecom industry trade group this week after a Wall Street Journal investigative report titled, “America Is Wrapped in Miles of Toxic Lead Cables.” The WSJ said it found evidence of more than 2,000 lead-covered cables and that there “are likely far more throughout the country.”

WSJ reporters had researchers collect samples as part of their investigation. They “found that where lead contamination was present, the amount measured in the soil was highest directly under or next to the cables, and dropped within a few feet—a sign the lead was coming from the cable,” the article said.

Markey wrote to USTelecom, “According to the Wall Street Journal’s investigation, ‘AT&T, Verizon and other telecom giants have left behind a sprawling network of cables covered in toxic lead that stretches across the US, under the water, in the soil and on poles overhead… As the lead degrades, it is ending up in places where Americans live, work and play.'”

Markey wants answers

Markey wants answers to a series of questions by July 25:

> *Do the companies know the locations and mileage of lead-*

> *sheathed cables that they own or for which they are responsible—whether aerial, underwater, or underground? Are there maps of the locations and installations? If not, what plans do the companies have to identify the cables?*
>
> *Why have the companies that knew about the cables—and the potential exposure risks they pose—failed to monitor them or act?*

Markey also asked what plans telcos have to address environmental and public health problems that could arise from lead cables. He asked the companies to commit to "testing for soil, water, and other contamination caused by the cables," to remediate any contamination, and warn communities of the potential hazards.

Markey also asked USTelecom if the phone companies will guarantee "medical treatment and compensation to anyone harmed by lead poisoning caused by the cables."

Advertisement

Markey isn't the only lawmaker expressing concern. "There is no safe level of lead exposure—*none*—which is why I'm so disturbed by these reports of lead cable lines throughout the country," US Rep. Frank Pallone Jr. (D-NJ) told the WSJ. "It is imperative that these cables be properly scrutinized and addressed."

Rep. Patrick Ryan (D-NY) told the Journal he is considering legislation on remediating contamination from the cables and that telecom companies should "do the right thing and clean up their mess." The Journal said its testing in a playground in Ryan's district "registered high levels of lead underneath an aerial cable running along the perimeter of the park."

A Light Reading article quoted New Street Research analysts as saying that "the WSJ article raises the prospects that the telephone companies may face significant financial exposure

down the road that the market has not anticipated” and that AT&T likely faces “the greatest exposure” due to the size of its network.

USTelecom: No cause for alarm

A USTelecom spokesperson told Ars today, “We are engaging with stakeholders on this important matter. The US telecom industry prioritizes the health and safety of our communities and workers. We have not seen, nor have regulators identified, evidence that legacy lead-sheathed telecom cables are a leading cause of lead exposure or the cause of a public health issue.”

USTelecom also set up a “Telecom Cable Facts” website to address concerns. “The use of lead alloys in telecom cables started in the 1880s and the industry began to phase out placement of new lead-sheathed cables in the 1950s after developing a new type of sheathing,” the trade group’s website said. “Some of these cables still provide customer voice and data services, including connecting 911 service, fire alarms, and other central monitoring stations.”

We contacted AT&T and Verizon today and will update this article if we get any response.

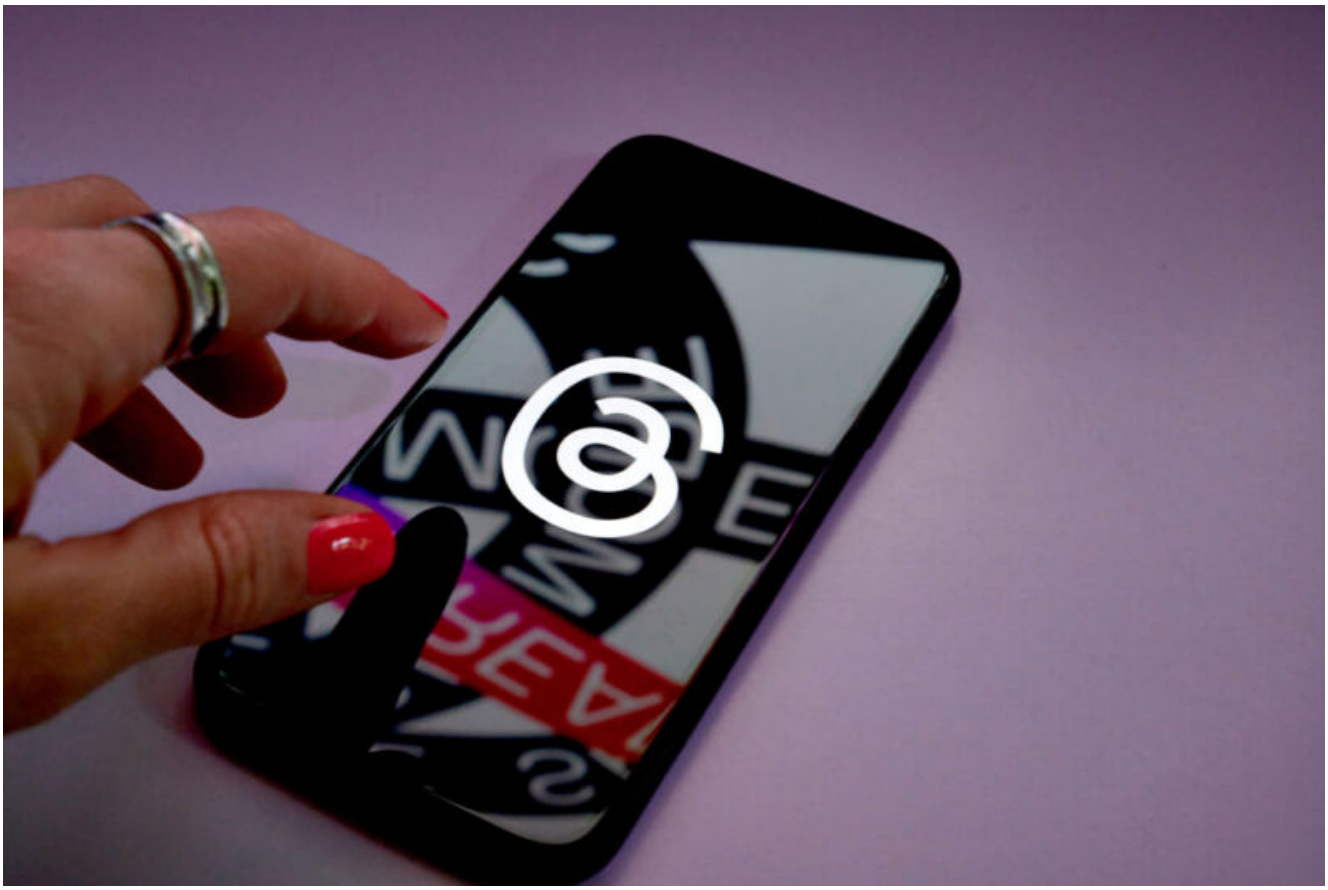
The WSJ reported, “For many years, telecom companies have known about the lead-covered cables and the potential risks of exposure to their workers, according to documents and interviews with former employees. They were also aware that lead was potentially leaching into the environment, but haven’t meaningfully acted on potential health risks to the surrounding communities or made efforts to monitor the cables.”

Markey’s letter called that passage from the article “especially concerning” and “corporate irresponsibility of the worst kind.” He said telecom companies have a “civil and

legal” duty to address the problem and promised that he will be “watching closely from my seats on Senate committees that have jurisdiction over the environmental and public health issues these cables present.” Markey is chair of the Senate Environment and Public Works Subcommittee on Clean Air, Climate, and Nuclear Safety.

https://arstechnica.com/?p=1954031

Threads usage drops as Meta blocks VPN access in EU [Updated]



reader comments

125 with

[Update: Top10VPN’s head of research, Simon Migliano, told Ars that “demand for VPN services is significantly up in a handful of major EU countries, such as Italy (26 percent), France (19 percent) and Sweden (20 percent), and up around 12 percent across the bloc as a whole since the launch of Threads on July 5 compared to the daily average over the 30 days prior. Other countries with significant spikes include Croatia (20 percent), Denmark (23 percent), Greece (22 percent) and Luxembourg (21 percent).” Compared to its neighbors, “privacy conscious” Germany’s VPN “demand is fairly flat” and only up by 5 percent, Migliano said.

Migliano also indicated that it seemed likely that Meta may not be blocking all VPN traffic.

“It’s understandable that Meta would try to block VPN traffic to Threads in the hope of improving their standing with EU regulators looking at their wider business model,” Migliano told Ars. “It does however feel like it’s more for PR purposes than a serious attempt to lock out all EU users keen enough to use a VPN to access Threads. While Meta may well have gone for the low-hanging fruit of blocking easy-to-identify IP ranges, such as those from data centres, it would be much more resource-intensive to identify and block obfuscated VPN traffic for example.”**]**

This month, Meta’s new Twitter-alternative Threads launched in 100 countries, but not in the European Union, due to potential conflicts between the app’s vast data collection and the EU’s strict data privacy laws. Immediately, reports emerged that some EU users persisted in downloading Threads anyway—by hiding their location and accessing the app via a virtual private network, or VPN.

Advertisement
Now, Meta has confirmed that it has taken measures to block VPN access to Threads in the EU.

“Threads is not currently available in most countries in Europe, and we’ve taken additional steps to prevent people based there from accessing it at this time,” a Meta spokesperson told TechCrunch. “Europe continues to be an incredibly important market for Meta, and we hope to make Threads available here in the future.”

Many EU Threads users have taken to Twitter to confirm that their access has indeed been cut off.

Ars could not immediately reach Meta for further comment.

Threads collects a lot of private information about its users, including health and financial data, precise location, search history, and browsing history, for the purpose of targeting ads. In the EU, not only does the General Data Protection Regulation require minimization of data collection for limited purposes, but the Digital Markets Act (DMA) was specifically designed to make it much harder for tech giants, known as gatekeepers, to track user activity to target ads. Meta could face fines of up to 10 percent of its global revenue for failing to comply with the DMA and up to 20 percent for repeat violations.

Meta was one of seven platforms designated as a potential gatekeeper under the DMA. Because of that, the European Commission has said its apps must comply with the DMA within six months of a quickly approaching September 6 deadline, when the EU plans to officially designate all gatekeepers.

Until Meta figures out how to bring its apps into compliance with the DMA, Threads will likely remain inaccessible to users in many European countries. This could stunt the app’s growth, which started off explosive but has since tapered off, according to data firms Sensor Tower and Similarweb.

Advertisement
Sensor Tower reported that on Monday and Tuesday this week, Threads' "number of daily active users were down about 20 percent from Saturday, and the time spent for [each] user was down 50 percent, from 20 minutes to 10 minutes," CNBC reported.

Similarweb's findings painted a slightly starker picture, reporting that daily active users were down by more than 25 percent from Threads' peak on July 7 to Monday. Like Sensor Tower, Similarweb also found that average usage time has fallen by 50 percent, "dropping from about 20 minutes on July 6 to just over 8 minutes on July 10," CNBC reported.

It's currently unclear how many EU users were accessing Threads during the app's peak, making it hard to determine how big an impact blocking VPN access in the EU has had on Threads' traffic. But Similarweb's senior insights manager, David Carr, told CNBC that he attributes the dropoff to a trend showing that, despite "intense" initial interest in Threads, "not every user has made a habit of visiting Threads as often as they might other social apps."

Meanwhile, Twitter's Elon Musk continues to claim that under Twitter's new metric measuring user seconds per day, Twitter usage is going up. That's despite reports that Twitter traffic was down while Threads' traffic surged.

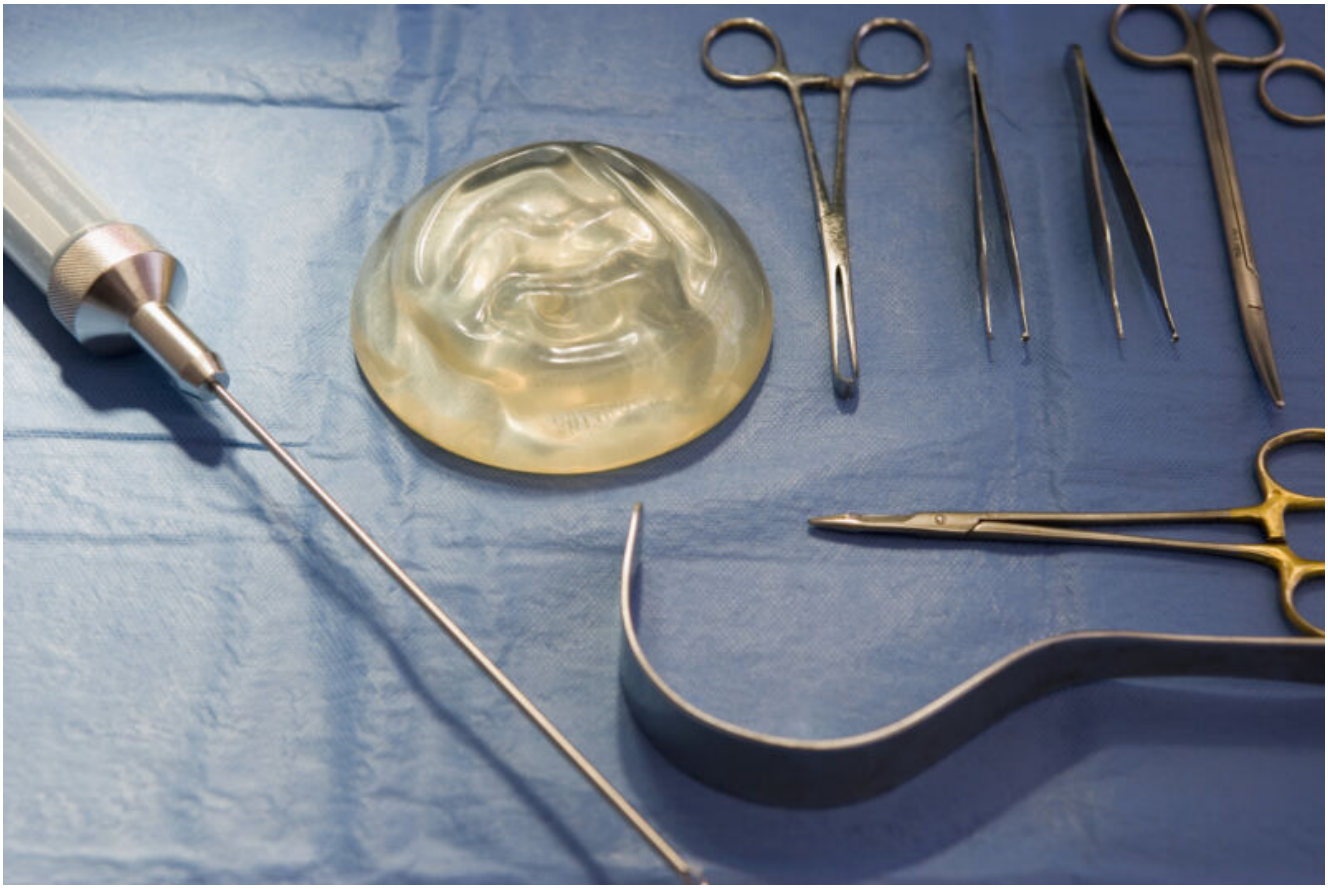
"Looks like this platform may see all-time high device user seconds usage this week," Musk tweeted.

While Threads gets a lot of heat over collecting a wide range of sensitive information—see how Threads' data collection compares with Twitter and other Twitter alternatives—a report from Top10VPN found that Threads "pales in comparison to Twitter when it comes to tracking its users across the Internet."

Top10VPN could not immediately be reached for comment.

https://arstechnica.com/?p=1953967

Ohio bans doctor after botched surgeries on TikTok threaten patients' lives



reader comments

32 with

Yesterday, an Ohio plastic surgeon, Katharine Grawe—who accumulated nearly 15 million likes by livestreaming operations on TikTok as "Doctor Roxy"—was permanently banned from practicing medicine and surgery in Ohio.

The decision came following a November 2022 suspension temporarily barring Grawe from seeing patients after the State Medical Board of Ohio reviewed “clear and convincing evidence” from multiple patients who were harmed during Grawe’s livestreamed surgeries. The board decided to suspend Grawe’s license, saying that her “continued practice presents a danger of immediate and serious harm to the public.”

The suspension notice details three anonymized patient complaints about “Doctor Roxy.” During one surgery that was livestreamed on TikTok, Grawe looked directly into the camera while inserting a thin tube called a cannula and performing liposuction on a patient.

“Despite liposuction being a blind surgery that requires awareness of the tip of the cannula to avoid injury, your attention to the camera meant at those moments you were not looking at the patient or palpating the location of the tip of the cannula,” the board wrote.

As a result of such negligence, that patient ended up needing a long hospital stay to deal with “free air in her abdomen,” a “perforated small bowel,” and a “necrotizing soft tissue infection,” the board wrote.

Another patient had to call 911 “due to cramping and severe abdominal pain” following a surgery involving a Brazilian butt lift, liposuction, and an umbilical hernia repair. That patient was rushed to the emergency room and had part of her small bowel removed after being diagnosed with a potentially fatal condition called rhabdomyolysis.

The third patient saw Grawe for a breast augmentation procedure involving silicone breast implants. In the days after that surgery, the patient felt nausea and noticed bleeding from the breast. The patient returned twice to Grawe’s office—Roxy Plastic Surgery—where Grawe delegated post-operation procedures to another surgeon and a nurse

practitioner despite the patient's "complex surgical history." Ultimately, the patient had to go to the hospital to have the implants removed—which the board said that Grawe "erroneously" indicated to the hospital's plastic surgeon had already happened.

Advertisement
"These outcomes were not normal complications like those that exist in the routine practice of medicine, but were rather caused by recklessness and disregard for the rules governing the practice of medicine in Ohio," Jonathan B. Feibel, vice president of the medical board, said during the board's hearing this week.

"Doctor Roxy" got two warnings

The board had warned Grawe twice before suspending her license of the potential ethical issues and their concerns about her departures from normal standards of care.

The first warning came in 2018 when the board told her that she needed "to maintain patient privacy when sharing photos or video via social media." On TikTok, Grawe shared "pre-operative photos, pre-operative interviews with patients about their bodies, livestreams of their procedures, post-operative still images of patients taken in the operating room, and the cost of the procedure," the board noted. Grawe also had a habit of responding "to viewers' online questions" during livestreams "while the surgical procedure" remained "actively ongoing," the board said.

Grawe responded to that warning by updating her patient consent form.

Her next warning came in September 2021, when the board "articulated multi-faceted issues" with Grawe's "care of these patients, including concerns regarding the lack of informed consent, ethical concerns related to privacy and social media,

and avoidable complications that required surgical revisions.”

At that point, the board recommended that Grawe “undertake remedial education courses related to complications of plastic surgery and professionalism/ethics.” Grawe complied by completing remedial education in “Ethical Social Media” and “Finesse in Mastopexy and Augmentation Mastopexy,” which only addressed patient complaints of surgeries to improve sagging of the breasts.

After that, she kept on posting videos to TikTok through October 2022, leading up to her suspension and yesterday’s decision to permanently revoke her medical license in Ohio. Feibel said during her hearing that Grawe had previously “dismissed complaints as coming from disgruntled former patients,” The Columbus Dispatch reported.

A spokesperson for the State Medical Board of Ohio, Jerica Stewart, told Ars that “a permanent revocation means Katharine Grawe will no longer be permitted to practice medicine and surgery in the State of Ohio.” Grawe was also fined “$4,500 based on her failure to meet standard of care,” Stewart said.

All actions taken are ultimately documented on the board’s website. Stewart said that once Grawe receives the final documents, the board’s order will also be available here.

Ars could not immediately reach Grawe or TikTok for comment. Grawe’s TikTok account remains active with more than 825,000 followers, but it is currently locked.

https://arstechnica.com/?p=1953654

Musk’s X Corp. sues data scrapers for “severely taxing” Twitter’s servers



Getty Images | Christopher Furlong

reader comments

188 with

Elon Musk’s X Corp. is suing four unidentified data scrapers accused of “severely tax[ing]” Twitter’s servers and degrading the social network’s user experience. The defendants, known only by their IP addresses so far, allegedly “engaged in widespread unlawful scraping of data from Twitter” by “flooding Twitter’s sign-up page with automated requests.”

“The volume of these requests far exceeded what any single

individual could send to a server in a given period and clearly indicated that these automated requests were aimed at scraping data from Twitter. These requests have severely taxed X Corp.’s servers and impaired the user experience for millions of X Corp.’s customers,” the lawsuit alleged.

The lawsuit, which seeks damages of at least $1 million, was filed last week in Dallas County District Court and reported yesterday by the Dallas-based station WFAA. The defendants are four John Does. Twitter hopes to learn their true identities during discovery.

The lawsuit was filed days after Twitter imposed rate limits on all users. “Several entities tried to scrape every tweet ever made in a short period of time. That is why we had to put rate limits in place,” Musk wrote in a tweet about the lawsuit.

X Corp. may be planning to sue other data scrapers in different geographical areas. The lawsuit said Twitter has identified more IP addresses as data scrapers but is suing these four in Dallas because they were “contracting with entities that maintain data processing facilities in Dallas County.”

Advertisement

X Corp. cites “massive demands” on servers

The lawsuit defines scraping as “a form of unauthorized data collection that uses automation and other processes to harvest data from a website or a mobile application.”

“Scraping interferes with the legitimate operation of websites and mobile applications, including Twitter, by placing millions of requests that tax the capacity of servers and impair the experience of actual users. Twitter users have no

control over how data-scraping companies repackage and sell their personal information," the complaint said.

Twitter prohibits scraping in its terms of service and "employs several technological measures designed to detect and prevent unauthorized scraping." Noting the recent rate limits, the lawsuit said the "massive demands on X Corp.'s servers from extremely aggressive data-scrapers" led it to impose "limits on how many Tweets each user could view in a given day. X Corp. has also limited access to Tweets for users who are not signed in to a registered Twitter account."

Twitter doesn't seem to know exactly what the scraped data was used for, but the lawsuit makes a claim for unjust enrichment and "seeks actual damages from Defendants' unlawful activities, an accounting, and disgorgement of Defendants' profits in an amount to be determined at trial."

Twitter is involved in a large number of lawsuits as both defendant and plaintiff. The company has been hit with more than 20 suits over allegedly unpaid bills for rent and various services, plus lawsuits from ex-employees and executives over unpaid severance, bonuses, and unpaid reimbursements.

Last week, X Corp. sued a law firm that Twitter hired last year after Musk tried to break their $44 billion merger agreement. Musk is trying to claw back $90 million that Twitter paid the firm. Musk's company also threatened to sue Meta, claiming that it used Twitter trade secrets to build its Twitter rival, Threads.

https://arstechnica.com/?p=1953629

FTC appeal in Microsoft/Activision case shows US regulator isn’t giving up yet



Artist’s conception of the FTC and Microsoft fighting over this deal in the courts.

reader comments

96 with

The Federal Trade Commission has given legal notice that it intends to appeal a recent district court decision that denied a temporary injunction in Microsoft’s proposed merger with Activision.

The appeal notice, filed with the 9th Circuit Court of Appeals late Wednesday, is a rare move for the FTC in cases like this. The FTC is facing down District Court Judge Jacqueline Scott

Corley's finding that the regulator "has not shown a likelihood it will prevail on its claim this particular vertical merger in this specific industry may substantially lessen competition."

An appeal would have to convince a circuit court judge of some key unconsidered area of fact or law to overturn that decision, which could be a high bar in this case. Still, the appeal filing itself shows that the FTC is not willing to give up easily in this high-profile case.

"The District Court's ruling makes crystal clear that this acquisition is good for both competition and consumers," Microsoft Vice Chair and President Brad Smith said in a statement to Ars Technica. "We're disappointed that the FTC is continuing to pursue what has become a demonstrably weak case, and we will oppose further efforts to delay the ability to move forward."

"The facts haven't changed," Activision Blizzard said in a statement. "We're confident the U.S. will remain among the 39 countries where the merger can close. We look forward to reinforcing the strength of our case in court, again."

Activision Blizzard CEO Bobby Kotick told CNBC earlier this week that he'd "be surprised if they would waste taxpayer resources on something like [an appeal]."

Advertisement
"Your tax dollars at work," Blizzard Entertainment President Mike Ybarra quipped on Twitter.

What comes next?

Microsoft is still subject to a temporary restraining order blocking it from closing the Activision deal, which was put in place to allow the previous district court proceedings to move forward. That order expires at the end of the day on Friday,

though, after which Microsoft and Activision could quickly move to finalize things before a contractual deadline of July 18. To prevent that possibility pending appeal, the FTC would have to apply for a separate emergency stay extending the restraining order.

Aside from the US, Microsoft and Activision still face opposition from the UK's Competition and Markets Authority (CMA), which blocked the deal in April over cloud gaming competition concerns. Following this week's decision in US courts, though, the CMA and Microsoft have jointly decided to stay continuing appeal litigation over that decision in order to negotiate "how the transaction might be modified in order to address those concerns in a way that is acceptable to the CMA."

That modification could involve a carve-out that prevents Microsoft from putting Activision games on its cloud service in the country. But the CMA warned in a Wednesday statement that negotiations with Microsoft are at "an early stage" and that its "final report still stands" as those negotiations move forward.

A Reuters analysis this month found that, in the past two years, the FTC has had a relatively low success rate in challenging vertical mergers like the Microsoft/Activision deal (where the companies involved fill different roles in the same broad industry). The FTC sued to block Quest-maker Meta from acquiring VR fitness company (and *Supernatural* maker) Within last July, but a judge ruled in February that the acquisition could move forward.

If the Activision acquisition is not closed before July 18, Microsoft is contractually on the hook for a $3 billion termination fee. But most observers expect both sides would simply extend the contract or renegotiate if closure seemed close at that point.

https://arstechnica.com/?p=1953562

Twitter is “tanking” amid Threads’ surging popularity, analysts say



reader comments

338 with

Data shows that a sudden spike in interest in Meta’s Threads—which surpassed 100 million sign-ups in five days, Mark Zuckerberg boasted yesterday—has likely already put a tiny dent in Twitter’s traffic, The Wall Street Journal

reported.

The news comes after a tweet from Cloudflare CEO Matthew Prince went viral. In it, Prince shared a Cloudflare chart showing that since January, Twitter traffic—compared to other popular websites—has been "tanking."

During Threads' first two days online, Twitter traffic dropped by 5 percent compared to the same two days in the prior week, web analytics firm SimilarWeb reported. When measuring year over year, Twitter's traffic dropped by 11 percent.

"We've been reporting for a while that Twitter is down compared with last year," David Carr, a SimilarWeb senior insights manager, told CNN. "But Threads seems to be taking a bigger bite out of it."

While Threads continued growing, Twitter execs Elon Musk and Linda Yaccarino started sharing a new metric for user engagement that they seemingly found more encouraging than the somewhat dismal traffic reports.

"Don't want to leave you hanging by a thread… but Twitter, you really outdid yourselves!" Yaccarino tweeted. "Last week we had our largest usage day since February."

Musk responded to that tweet, clarifying what Yaccarino meant by "usage."

"Cumulative user-seconds per day of phone screentime, as reported by iOS & Android, is hardest to game," Musk tweeted. "I think we may hit an all-time record this week."

Advertisement
While many Twitter users debated whether this new metric was meaningful—and some claimed it wasn't even possible to track—the T(w)itter Daily account explained "why Elon changed Twitter's metrics" from tracking monthly daily active users (mDAU) to user-seconds per day.

“The old mDAU metric” included bots and “people who got a Twitter notification on their phone but didn’t open the app,” while the “new metric is much harder to manipulate,” T(w)itter Daily tweeted.

T(w)itter Daily also claimed that Twitter 2.0 data scientists had verified that “despite some claims to the contrary, it absolutely is possible for Twitter to track how much time people use the app on iOS and Android.”

Musk responded to T(w)itter Daily’s thread, confirming that bots can still manipulate the new metric “via humans with lots of phones, but that is [more than] 100 times more expensive than bots.”

Right now, CNN reported that Threads is “on pace to rapidly pass Twitter’s audience size.” Both SimilarWeb and Cloudflare told CNN that Twitter traffic trending downward appears to have been accelerated by Threads’ launch, which seems to pose an obvious risk to Twitter’s business. It’s possible that Yaccarino’s and Musk’s tweets have introduced a new metric in an effort to reassure advertisers that Twitter engagement has gone up, despite reports of traffic tanking.

T(w)itter Daily went so far as to claim that the reason that Twitter user activity is up despite Threads launching—and despite its own decision to start rate-limiting tweets—is because “all publicity is good publicity.” Following that logic, all reports comparing Threads’ success to Twitter’s decline, including this one (which links to multiple tweets), ultimately lead Twitter users back to Twitter.

Meta and Twitter did not immediately respond to Ars’ request to comment.

https://arstechnica.com/?p=1952925

Sarah Silverman sues OpenAI, Meta for being “industrial-strength plagiarists”



Enlarge / Comedian and author Sarah Silverman.

reader comments

338 with

On Friday, the Joseph Saveri Law Firm filed US federal class-action lawsuits on behalf of Sarah Silverman and other authors against OpenAI and Meta, accusing the companies of illegally

using copyrighted material to train AI language models such as ChatGPT and LLaMA.

Other authors represented include Christopher Golden and Richard Kadrey, and an earlier class-action lawsuit filed by the same firm on June 28 included authors Paul Tremblay and Mona Awad. Each lawsuit alleges violations of the Digital Millennium Copyright Act, unfair competition laws, and negligence.

The Joseph Saveri Law Firm is no stranger to press-friendly legal action against generative AI. In November 2022, the same firm filed suit over GitHub Copilot for alleged copyright violations. In January 2023, the same legal group repeated that formula with a class-action lawsuit against Stability AI, Midjourney, and DeviantArt over AI image generators. The GitHub lawsuit is currently on path to trial, according to lawyer Matthew Butterick. Procedural maneuvering in the Stable Diffusion lawsuit is still underway with no clear outcome yet.

In a press release last month, the law firm described ChatGPT and LLaMA as “industrial-strength plagiarists that violate the rights of book authors.” Authors and publishers have been reaching out to the law firm since March 2023, lawyers Joseph Saveri and Butterick wrote, because authors “are concerned” about these AI tools’ “uncanny ability to generate text similar to that found in copyrighted textual materials, including thousands of books.”

The most recent lawsuits from Silverman, Golden, and Kadrey were filed in a US district court in San Francisco. Authors have demanded jury trials in each case and are seeking permanent injunctive relief that could force Meta and OpenAI to make changes to their AI tools.

Meta declined Ars’ request to comment. OpenAI did not immediately respond to Ars’ request to comment.

A spokesperson for the Saveri Law Firm sent Ars a statement,

saying, “If this alleged behavior is allowed to continue, these models will eventually replace the authors whose stolen works power these AI products with whom they are competing. This novel suit represents a larger fight for preserving ownership rights for all artists and other creators.”

Accused of using “flagrantly illegal” data sets

Neither Meta nor OpenAI has fully disclosed what’s in the data sets used to train LLaMA and ChatGPT. But lawyers for authors suing say they have deduced the likely data sources from clues in statements and papers released by the companies or related researchers. Authors have accused both OpenAI and Meta of using training data sets that contained copyrighted materials distributed without authors’ or publishers’ consent, including by downloading works from some of the largest e-book pirate sites.

In the OpenAI lawsuit, authors alleged that based on OpenAI disclosures, ChatGPT appeared to have been trained on 294,000 books allegedly downloaded from “notorious ‘shadow library’ websites like Library Genesis (aka LibGen), Z-Library (aka Bok), Sci-Hub, and Bibliotik.” Meta has disclosed that LLaMA was trained on part of a data set called ThePile, which the other lawsuit alleged includes “all of Bibliotik,” and amounts to 196,640 books.

On top of allegedly accessing copyrighted works through shadow libraries, OpenAI is also accused of using a “controversial data set” called BookCorpus.

BookCorpus, the OpenAI lawsuit said, “was assembled in 2015 by a team of AI researchers for the purpose of training language models.” This research team allegedly “copied the books from a website called Smashwords that hosts self-published novels,

that are available to readers at no cost." These novels, however, are still under copyright and allegedly "were copied into the BookCorpus data set without consent, credit, or compensation to the authors."

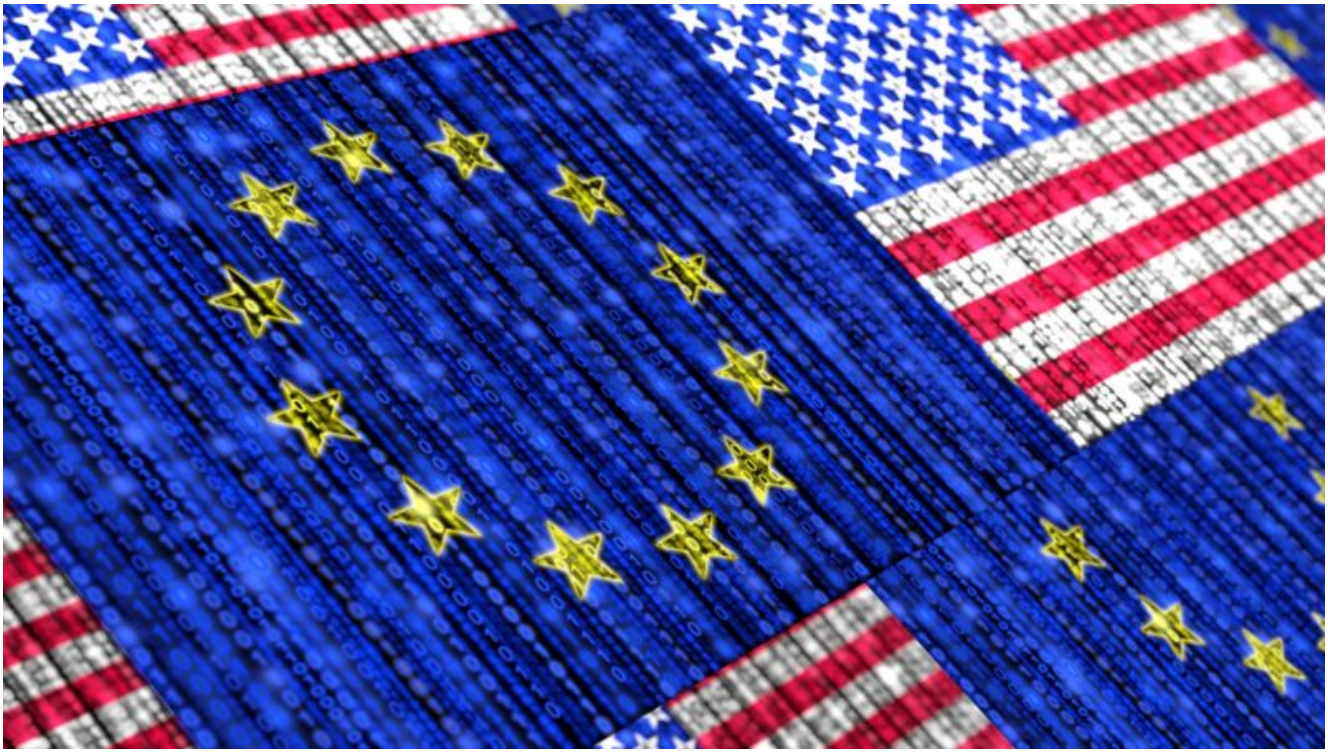
Ars could not immediately reach the BookCorpus researchers or Smashwords for comment. [**Update:** Dan Wood, COO of Draft2Digital—which acquired Smashwords in March 2022—told Ars that the Smashwords "store site lists close to 800,000 titles for sale," with "about 100,000" currently priced at free.

"Typically, the free book will be the first of a series," Wood said. "Some authors will keep these titles free indefinitely, and some will run limited promotions where they offer the book for free. From what we understand of the BookCorpus data set, approximately 7,185 unique titles that were priced free at the time were scraped without the knowledge or permission of Smashwords or its authors." It wasn't until March 2023 when Draft2Digital "first became aware of the scraped books being used for commercial purposes and redistributed, which is a clear violation of Smashwords' terms of service," Wood said.

"Every author, whether they have an internationally recognizable name or have just published their first book, deserve to have their copyright protected," Wood told Ars. "They also should have the confidence that the publishing service they entrust their work with will protect it. To that end, we are working diligently with our lawyers to fully understand the issues—including who took the data and where it was distributed—and to devise a strategy to ensure our authors' rights are enforced. We are watching the current cases being brought against OpenAI and Meta very closely."]

https://arstechnica.com/?p=1952424

Big Tech can transfer Europeans' data to US in win for Facebook and Google



Getty Images | BeeBright

reader comments

62 with

The European Commission today decided it is safe for personal data to be transferred from the European Union to US-based companies, handing a victory to firms like Facebook and Google despite protests from privacy advocates who worry about US government surveillance.

The commission announced that it "adopted its adequacy decision for the EU-US Data Privacy Framework," concluding "that the United States ensures an adequate level of protection—comparable to that of the European Union—for personal data transferred from the EU to US companies under

the new framework. On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards."

In May, Facebook-owner Meta was fined 1.2 billion euros for violating the General Data Protection Regulation (GDPR) with transfers of personal data to the United States and was ordered to stop storing European Union user data in the US within six months. But Meta said at the time that if the pending data-transfer pact "comes into effect before the implementation deadlines expire, our services can continue as they do today without any disruption or impact on users."

The data-transfer deal "is expected to face a legal challenge from European privacy advocates, who have long said that the US needs to make substantial changes to surveillance laws," a Wall Street Journal report said today. "Transfers of data from Europe to the US have been in question since an EU court ruled in 2020 that a previous deal allowing trans-Atlantic data flows was illegal because the US didn't give EU individuals an effective way to challenge surveillance of their data by the US government."

US to monitor compliance

The EC's announcement said the new framework has "binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access." The new court "will be able to order the deletion" of data that is found to have been collected in violation of the new rules.

Advertisement

The framework will be administered and monitored by the US Department of Commerce and the "US Federal Trade Commission

will enforce US companies' compliance," the EC announcement said. EU residents who challenge data collection will have free access to "independent dispute resolution mechanisms and an arbitration panel."

The US and EC agreed on the data privacy framework in March 2022, and the US announced last week that it has fulfilled its commitments for implementing the deal.

Google supported the agreement, writing last year that the "US government has now committed to systems that will enable independent and meaningful redress for people in the EU, strengthen the guardrails and proportionality of US intelligence collection, and ensure effective oversight of these new privacy and civil liberties standards in ways that address the concerns articulated by the Court of Justice of the European Union." Google also said the agreement provides "a reliable and durable foundation for the future of Internet services on both sides of the Atlantic."

US companies can join the EU-US framework "by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties," the European Commission said.

Privacy activist plans appeal

Previous data agreements known as Safe Harbor and Privacy Shield were struck down by European courts, the WSJ noted. "Max Schrems, an Austrian lawyer and privacy activist who led the legal challenges to the earlier agreements, said he plans to challenge the latest deal, too," the report said.

"We would need changes in US surveillance law to make this work and we simply don't have it," Schrems was quoted as saying.

European Parliament member Birgit Sippel, who is in Germany's Social Democratic Party, said the "framework does not provide any meaningful safeguards against indiscriminate surveillance conducted by US intelligence agencies," according to The New York Times.

The EC approval of the deal was lauded by the Computer & Communications Industry Association, which represents Amazon, Apple, eBay, Google, Meta, Twitter, and other tech companies. "Today's decision means that EU and US businesses will soon have full legal certainty again to transfer personal data across the Atlantic… Data flows are vital to transatlantic trade and the EU-US economic relationship, which is worth €5.5 trillion per year. Nevertheless, the two economies had been left without guidelines for data transfers after an EU Court ruling invalidated the previous framework back in 2020," the group said.

https://arstechnica.com/?p=1952570

Musk sues law firm because he's mad that Twitter paid $90 million bill



Aurich Lawson / Duncan Hull / Getty

reader comments

321 with

Elon Musk’s X Corp. this week sued a law firm that Twitter hired last year after Musk tried to break their $44 billion merger agreement. Musk’s lawsuit in San Francisco County Superior Court alleges that Wachtell, Lipton, Rosen & Katz overcharged Twitter when it collected $90 million—including $84.3 million on the same day Musk completed his purchase of Twitter.

“This action for equitable relief arises out of an effort by Wachtell to fundamentally alter its fee arrangement as litigation counsel in the twilight of its representation of Twitter to obtain an improper bonus payment in violation of its fiduciary and ethical obligations to its client,” claimed the lawsuit filed by X Corp., the successor company to Twitter. “Wachtell exploited a corporate client left unprotected by lame duck fiduciaries who had lost their motivation to act in Twitter’s best interest pending its

imminent sale to Elon Musk and his entities, X Holdings I, Inc. and X Holdings II, Inc.”

When Musk tried to pull out of his commitment to buy Twitter, the company hired Wachtell in July 2022 to handle the lawsuit that eventually forced Musk to complete the merger. Musk finally honored the merger contract in October when it became clear that he would likely lose in court.

The Musk/Twitter deal closed on October 27. Wachtell allegedly charged Twitter $90 million for several months of work, with $84.3 million being paid on the day the merger closed. The $90 million fee included earlier invoices totaling nearly $18 million, the lawsuit said.

“Fully aware that nobody with an economic interest in Twitter’s financial well-being was minding the store, Wachtell arranged to effectively line its pockets with funds from the company cash register while the keys were being handed over to the Musk Parties,” Musk’s lawsuit said.

Musk’s Twitter apparently hasn’t paid many bills since then, as the company is facing more than 20 lawsuits over allegedly unpaid bills for rent and various services. Twitter is also facing lawsuits from ex-employees over unpaid severance and bonuses, and a lawsuit from former CEO Parag Agrawal and other ex-executives over unpaid reimbursements.

$84.3 million mostly a “success fee”

The bulk of the $84.3 million paid to Wachtell on October 27 was allegedly a “success fee” for forcing Musk to close the deal. Musk’s lawsuit said it “is impossible to determine what portion of the $90 million total fee due to Wachtell under the Closing Day Letter Agreement represents the referenced success fee.” Based on other invoices and accrued fees, the success

fee is said to be either $61 million or $72 million.

Advertisement

The X Corp. lawsuit describes how the payment was allegedly approved and paid before Musk could stop it:

> *In the middle of the board's final October 27 meeting, former Twitter general counsel Sean Edgett sent the chart of fees that the Twitter board was meeting to approve. Upon seeing the magnitude of the fees being presented for the board's approval, one former Twitter director immediately exclaimed in an email reply to Edgett:*
>
> *O*
>
> *My*
>
> *Freaking*
>
> *God*
>
> *Despite any initial shock, Twitter's lame duck board members voted to approve Wachtell's excessive and unconscionable fee.*
>
> *Immediately following the Twitter board's rubber-stamp approval, [Chief Legal Officer Vijaya] Gadde signed Wachtell's letter agreement. Then, to ensure that the eleventh-hour fee payment went through before the Musk Parties (Twitter's new owners) could learn about the massive gift included in that fee, Edgett expedited the wire payment on the invoice for the balance ($84,294,962.97) of the $90 million total fee that Wachtell had submitted to Twitter the day before. Twitter's $84 million wire to Wachtell was posted only ten minutes before Gadde and Edgett were terminated upon the closing of the merger.*

Wachtell has previously represented Musk and Tesla in other matters.

Musk asks for full $90 million

The lawsuit accuses Wachtell of unjust enrichment, breach of fiduciary duty, aiding and abetting breach of fiduciary duty, and violations of California's Business & Professions Code. We contacted Wachtell, Lipton, Rosen & Katz today and will update this article if we get a response.

"Due to its egregious violations of its professional duties and applicable ethical rules, Wachtell should be required to forfeit its entire $90 million total fee under the Closing Day Letter Agreement and make restitution in the amount of $90 million," the lawsuit said.

If the court doesn't require Wachtell to forfeit the entire fee, Musk argues that it "should be ordered to make restitution for the difference between the $90 million total fee it received and the reasonable fees it would have received had it adhered to the billing guidelines it agreed upon in the June 21 Engagement Letter."

Wachtell originally "signed an engagement letter for an hourly fee representation" but "failed to obtain a written agreement for any fee tied to the results of the underlying case," Musk's lawsuit alleges. The last-minute success fee indicates that "Wachtell apparently believed that it—unlike other law firms bound by ethical and fiduciary obligations—was free to solicit a handout, aid and abet corporate waste by former Twitter executives in the death throes of their fiduciary roles, and walk away with a total fee that made it $90 million richer," the lawsuit said.

https://arstechnica.com/?p=1952281