Mark Zuckerberg’s illegal school drove his neighbors crazy



Fox said that the Zuckerbergs instituted “a revised parking policy late last year” that should address their concerns, and promised to double down on efforts to give advanced notice about construction, parties, and other potential disruptions.

However, Fox did not directly address the unpermitted school and other nonresidential activities happening at the compound. She acknowledged that the compound has “residential support staff” including “childcare, culinary, personal assistants, property management, and security,” but said that they have “policies in place to minimize their impact on the neighborhood.”

It’s unclear if the neighbor responded to Fox.

“You have not earned our trust”

While these conversations were happening between Fox and Zuckerberg’s neighbors, Lait and others at the city Planning Department were scrambling to find a solution for the neighbor who complained on September 11, and a few other neighbors who endorsed the complaint in September and February.

Starting in February, one of these neighbors took the lead on following up with Lait. They asked him for an update on February 11, and heard back a few days later. He didn’t have any major updates, “but after conversations with the family’s representatives, he said he was exploring whether a “subset of children” could continue to come to the school sometimes for “ancillary” uses.

“I also believe a more nuanced solution is warranted in this case,” Lait added. Ideally, such a solution would respond to the neighbors’ complaints, but allow the Zuckerbergs to “reasonably be authorized by the zoning code.”

The neighbor wasn’t thrilled. The next day, they replied and called the city’s plan “unsatisfactory.”

“The city’s ‘nuanced solution’ in dealing with this serial violator has led to the current predicament,” they said (referring to the nuanced solution Lait mentioned in his last email.)

Horrigan-Taylor, the Palo Alto spokesperson, told WIRED that Lait’s mention of a “nuanced” solution referred to “resolving, to the extent permissible by law, neighborhood impacts and otherwise permitted use established by state law and local zoning.”

https://arstechnica.com/tech-policy/2025/11/mark-zuckerbergs-illegal-school-drove-his-neighbors-crazy/

Elon Musk wins $1 trillion Tesla pay vote despite “part-time CEO” criticism



Tesla shareholders today voted to approve a compensation plan that would pay Elon Musk more than $1 trillion over the next decade if he hits all of the plan’s goals. Musk won over 75 percent of the vote, according to the announcement at today’s shareholder meeting.

The pay plan would give Musk 423,743,904 shares, awarded in 12 tranches of 35,311,992 shares each if Tesla achieves various operational goals and market value milestones. Goals include delivering 20 million vehicles, obtaining 10 million Full Self-Driving subscriptions, delivering 1 million “AI robots,” putting 1 million robotaxis in operation, and achieving a $400 billion adjusted EBITDA (earnings before interest, taxes, depreciation, and amortization).

Musk has threatened to leave if he doesn’t get a larger share of Tesla. He told investors last month, “It’s not like I’m going to go spend the money. It’s just, if we build this robot army, do I have at least a strong influence over that robot army? Not control, but a strong influence. That’s what it comes down to in a nutshell. I don’t feel comfortable building that robot army if I don’t have at least a strong influence.”

The plan has 12 market capitalization milestones topping out at $8.5 trillion. The value of Musk’s award is estimated to exceed $1 trillion if he hits all operational and market capitalization goals. Musk would increase his ownership stake to 24.8 percent of Tesla, or 28.8 percent if Tesla ends up winning an appeal in the court case that voided his 2018 pay plan.

Tesla Chair Robyn Denholm has argued that Musk needs big pay packages to stay motivated. Some investors have said $1 trillion is too much for a CEO who spends much of his time running other companies such as SpaceX, X (formerly Twitter), and xAI.

New York Comptroller Thomas DiNapoli, who runs a state retirement fund that owns over 3.3 million shares, slammed the pay plan in a webinar last week. He said that Musk’s existing stake in Tesla should already “be incentive enough to drive performance. The idea that another massive equity award will somehow refocus a man who is hopelessly distracted is both illogical and contrary to the evidence. This is not pay for performance; this is pay for unchecked power.”

Musk and his side hustles

With Musk spending more time at xAI, “some major Tesla investors have privately pressed top executives and board members about how much attention Musk was actually paying to the company and about whether there is a CEO succession plan,” a Wall Street Journal article on Tuesday said. “An unusually

large contingent of Tesla board members, including chair Robyn Denholm, former Chipotle CFO Jack Hartung and Tesla co-founder JB Straubel, met with big investors in New York last week to advocate for Musk’s proposed new pay package.”

https://arstechnica.com/tech-policy/2025/11/elon-musk-wins-tesla-pay-vote-that-could-make-him-a-1-trillion-man/

DHS offers “disturbing new excuses” to seize kids’ biometric data, expert says



Civil and digital rights experts are horrified by a proposed rule change that would allow the Department of Homeland Security to collect a wide range of sensitive biometric data on all immigrants, without age restrictions, and store that data throughout each person’s “lifecycle” in the immigration

system.

If adopted, the rule change would allow DHS agencies, including Immigration and Customs Enforcement (ICE), to broadly collect facial imagery, finger and palm prints, iris scans, and voice prints. They may also request DNA, which DHS claimed "would only be collected in limited circumstances," like to verify family relations. These updates would cost taxpayers $288.7 million annually, DHS estimated, including $57.1 million for DNA collection alone. Annual individual charges to immigrants submitting data will likely be similarly high, estimated at around $231.5 million.

Costs could be higher, DHS admitted, especially if DNA testing is conducted more widely than projected.

"DHS does not know the full costs to the government of expanding biometrics collection in terms of assets, process, storage, labor, and equipment," DHS's proposal said, while noting that from 2020 to 2024, the US only processed such data from about 21 percent of immigrants on average.

Alarming critics, the update would allow DHS for the first time to collect biometric data of children under 14, which DHS claimed would help reduce human trafficking and other harms by making it easier to identify kids crossing the border unaccompanied or with a stranger.

Jennifer Lynch, general counsel for a digital rights nonprofit called the Electronic Frontier Foundation, told Ars that EFF joined Democratic senators in opposing a prior attempt by DHS to expand biometric data collection in 2020.

There was so much opposition to that rule change that DHS ultimately withdrew it, Lynch noted, but DHS confirmed in its proposal that the agency expects more support for the much broader initiative under the current Trump administration. Quoting one of Trump's earliest executive orders in this term, directing DHS to "secure the border," DHS suggested it was the

agency’s duty to use “any available technologies and procedures to determine the validity of any claimed familial relationship between aliens encountered or apprehended by the Department of Homeland Security.”

https://arstechnica.com/tech-policy/2025/11/dhs-wants-to-use-biometrics-to-track-immigrant-kids-throughout-their-lives/

Flock haters cross political divides to remove error-prone cameras



“People should care because this could be you,” White said. “This is something that police agencies are now using to document and watch what you’re doing, where you’re going,

without your consent.”

Haters cross political divides to fight Flock

Currently, Flock’s reach is broad, “providing services to 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states,” lawmakers noted. Additionally, in October, Flock partnered with Amazon, which allows police to request Ring camera footage that widens Flock’s lens further.

However, Flock’s reach notably doesn’t extend into certain cities and towns in Arizona, Colorado, New York, Oregon, Tennessee, Texas, and Virginia, following successful local bids to end Flock contracts. These local fights have only just started as groups learn from each other, Sarah Hamid, EFF’s director of strategic campaigns, told Ars.

“Several cities have active campaigns underway right now across the country—urban and rural, in blue states and red states,” Hamid said.

A Flock spokesperson told Ars that the growing effort to remove cameras “remains an extremely small percentage of communities that consider deploying Flock technology (low single digital percentages).” To keep Flock’s cameras on city streets, Flock attends “hundreds of local community meetings and City Council sessions each month, and the vast majority of those contracts are accepted,” Flock’s spokesperson said.

Hamid challenged Flock’s “characterization of camera removals as isolated incidents,” though, noting “that doesn’t reflect what we’re seeing.”

“The removals span multiple states and represent different organizing strategies—some community-led, some council-initiated, some driven by budget constraints,” Hamid said.

Most recently, city officials voted to remove Flock cameras this fall in Sedona, Arizona.

A 72-year-old retiree, Sandy Boyce, helped fuel the local movement there after learning that Sedona had “quietly” renewed its Flock contract, NBC News reported. She felt enraged as she imagined her tax dollars continuing to support a camera system tracking her movements without her consent, she told NBC News.

https://arstechnica.com/tech-policy/2025/11/flock-haters-cross-political-divides-to-remove-error-prone-cameras/

US gives local police a face-scanning app similar to one used by ICE agents



“Biometric data used to identify individuals through TVS are collected by government authorities consistent with the law, including [when] issuing documents or processing illegal aliens,” the CBP statement said. “The Mobile Fortify Application provides a mobile capability that uses facial comparison as well as fingerprint matching to verify the identity of individuals against specific immigration related holdings.”

404 Media quoted Cooper Quintin, senior staff technologist at the Electronic Frontier Foundation, as saying that “face surveillance in general, and this tool specifically, was already a dangerous infringement of civil liberties when in the hands of ICE agents. Putting a powerful surveillance tool like this in the hands of state and local law enforcement officials around the country will only further erode peoples’ Fourth Amendment rights, for citizens and non-citizens alike. This will further erode due process, and subject even more Americans to omnipresent surveillance and unjust detainment.”

DHS proposes new biometrics rules, definition

In related news this week, the Department of Homeland Security is proposing rule changes to expand the collection and use of biometric information. The proposed changes are open for public comment until January 2, 2026.

“The purpose of this rule is to establish a standard and provide notice that every individual filing or associated with a benefit request, other request, or collection of information is subject to the biometrics requirement, unless DHS exempts a category of requests or individuals, or a specific individual,” the proposal said. “This includes any alien apprehended, arrested or encountered by DHS in the course of performing its functions related to administering and enforcing the immigration and naturalization laws of the

United States. As it relates to benefit requests, other requests and collections of information, notice of this requirement will be added in the form instructions for the relevant forms, as needed.”

The proposed rule change would expand the agency’s definition of biometrics “to include a wider range of modalities than just fingerprints, photographs and signatures.” The proposed definition of biometrics is “measurable biological (anatomical, physiological or molecular structure) or behavioral characteristics of an individual.” This includes face and eye scans, vocal signatures, and DNA.

https://arstechnica.com/tech-policy/2025/11/us-gives-local-police-a-face-scanning-app-similar-to-one-used-by-ice-agents/

Real humans don’t stream Drake songs 23 hours a day, rapper suing Spotify says



“Spotify in no way benefits from the industry-wide challenge of artificial streaming,” Spotify’s spokesperson said. “We heavily invest in always-improving, best-in-class systems to combat it and safeguard artist payouts with strong protections like removing fake streams, withholding royalties, and charging penalties.”

Fake fans appear to move hundreds of miles between plays

Spotify has publicly discussed ramping up efforts to detect and penalize streaming fraud. But RBX alleged that instead, Spotify “deliberately” “deploys insufficient measures to address fraudulent streaming,” allowing fraud to run “rampant.”

The platform appears least capable at handling so-called “Bot Vendors” that “typically design Bots to mimic human behavior and resemble real social media or streaming accounts in order to avoid detection,” the lawsuit alleged.

These vendors rely on virtual private networks (VPNs) to

obscure locations of streams, but “with reasonable diligence,” Spotify could better detect them, RBX alleged—especially when streams are coming “from areas that lack the population to support a high volume of streams.”

For example, RBX again points to Drake’s streams. During a four-day period in 2024, “at least 250,000 streams of Drake’s song ‘No Face’ originated in Turkey but were falsely geomapped through the coordinated use of VPNs to the United Kingdom,” the lawsuit alleged, based on “information and belief.”

Additionally, “a large percentage of the accounts streaming Drake’s music were geographically concentrated around areas whose populations could not support the volume of streams emanating therefrom. In some cases, massive amounts of music streams, more than a hundred million streams, originated in areas with zero residential addresses,” the lawsuit alleged.

Just looking at how Drake’s fans move should raise a red flag, RBX alleged:

> *“Geohash data shows that nearly 10 percent of Drake’s streams come from users whose location data showed that they traveled a minimum of 15,000 kilometers in a month, moved unreasonable locations between songs (consecutive plays separated by mere seconds but spanning thousands of kilometers), including more than 500 kilometers between songs (roughly the distance from New York City to Pittsburgh).”*

Spotify could cut off a lot of this activity, RBX alleged, by ending its practice of allowing free ad-supported accounts to sign up without a credit card. But supposedly it doesn’t, because “Spotify has an incentive for turning a blind eye to the blatant streaming fraud occurring on its service,” the lawsuit said.

https://arstechnica.com/tech-policy/2025/11/real-humans-dont-stream-drake-songs-23-hours-a-day-rapper-suing-spotify-says/

Trump on why he pardoned Binance CEO: “Are you ready? I don’t know who he is.”



“My sons are involved in crypto much more than I—me,” Trump said on *60 Minutes*. “I—I know very little about it, other than one thing. It’s a huge industry. And if we’re not gonna be the head of it, China, Japan, or someplace else is. So I am behind it 100 percent.”

Did Trump ever meet Zhao? Did he form his own opinion about Zhao’s conviction, or was he merely “told about it”? Trump doesn’t seem to know:

> *This man was treated really badly by the Biden administration. And he was given a jail term. He’s highly respected. He’s a very successful guy. They sent him to jail and they really set him up. That’s my opinion. I was told*

> *about it.*
>
> *I said, “Eh, it may look bad if I do it. I have to do the right thing.” I don’t know the man at all. I don’t think I ever met him. Maybe I did. Or, you know, somebody shook my hand or something. But I don’t think I ever met him. I have no idea who he is. I was told that he was a victim, just like I was and just like many other people, of a vicious, horrible group of people in the Biden administration.*

Trump: “A lot people say that he wasn’t guilty”

Pointing out that Trump’s pardon of Zhao came after Binance helped facilitate a $2 billion purchase of World Liberty’s stablecoin, O’Donnell asked Trump to address the appearance of a pay-to-play deal.

“Well, here’s the thing, I know nothing about it because I’m too busy doing the other… I can only tell you this. My sons are into it. I’m glad they are, because it’s probably a great industry, crypto. I think it’s good… I know nothing about the guy, other than I hear he was a victim of weaponization by government. When you say the government, you’re talking about the Biden government. It’s a corrupt government. Biden was the most corrupt president and he was the worst president we’ve ever had.”

https://arstechnica.com/tech-policy/2025/11/trump-on-why-he-pardoned-binance-ceo-are-you-ready-i-dont-know-who-he-is/

Internet Archive's legal fights are over, but its founder mourns what was lost



With governments globally partnering with the biggest tech companies to try to win the artificial intelligence race, critics have warned of threats to US democracy, while the White House has escalated its attack on libraries, universities, and science over the past year.

Meanwhile, AI firms face dozens of lawsuits from creators and publishers, which Kahle thinks only the biggest tech companies can likely afford to outlast. The momentum behind AI risks giving corporations even more control over information, Kahle said, and it's uncertain if archives dedicated to preserving the public memory will survive attacks from multiple fronts.

"Societies that are [growing] are the ones that need to educate people" and therefore promote libraries, Kahle said. But when societies are "going down," such as in times of war, conflict, and social upheaval, libraries "tend to get

destroyed by the powerful. It used to be king and church, and it’s now corporations and governments.” (He recommended *The Library: A Fragile History* as a must-read to understand the challenges libraries have always faced.)

Kahle told Ars he’s not “black and white” on AI, and he even sees some potential for AI to enhance library services.

He’s more concerned that libraries in the US are losing support and may soon cease to perform classic functions that have always benefited civilizations—like buying books from small publishers and local authors, supporting intellectual endeavors, and partnering with other libraries to expand access to diverse collections.

To prevent these cultural and intellectual losses, he plans to position IA as a refuge for displaced collections, with hopes to digitize as much as possible while defending the early dream that the Internet could equalize access to information and supercharge progress.

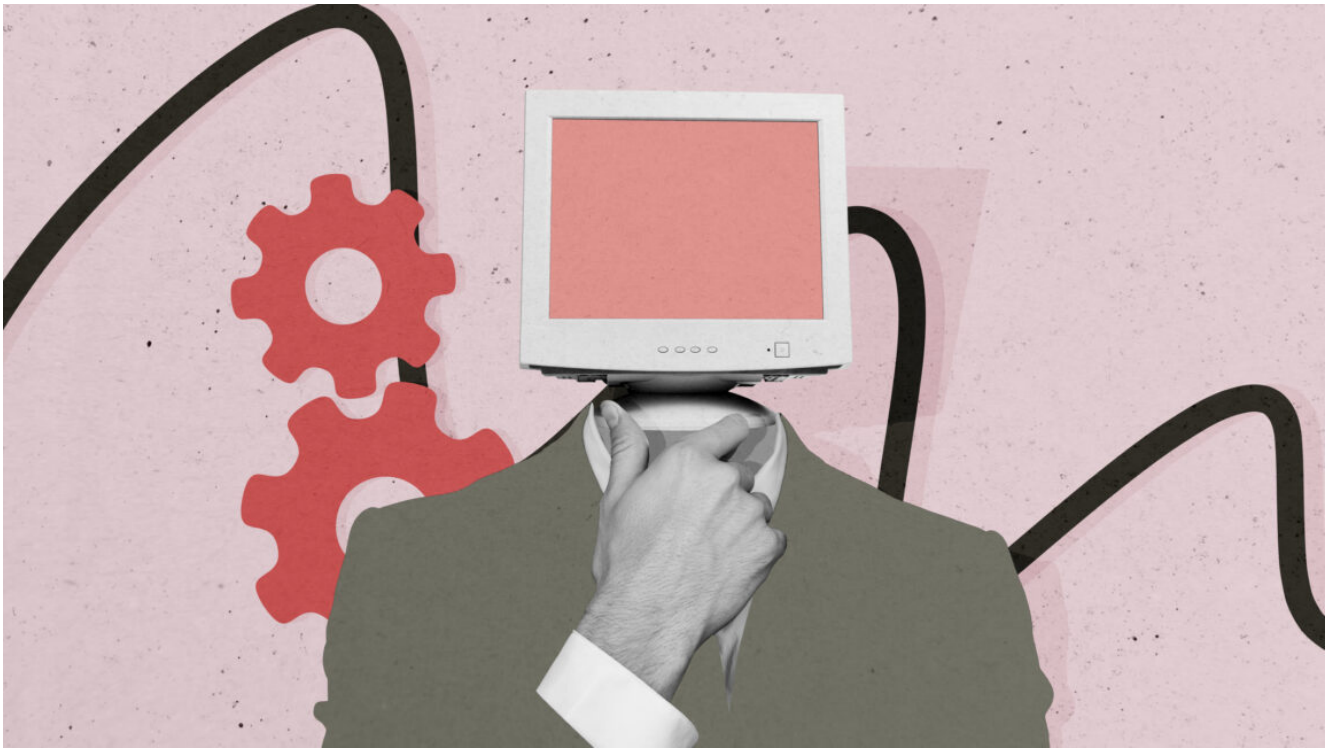
“We want everyone [to be] a reader,” Kahle said, and that means “we want lots of publishers, we want lots of vendors, booksellers, lots of libraries.”

But, he asked, “Are we going that way? No.”

To turn things around, Kahle suggested that copyright laws be “re-architected” to ensure “we have a game with many winners”—where authors, publishers, and booksellers get paid, library missions are respected, and progress thrives. Then society can figure out “what do we do with this new set of AI tools” to keep the engine of human creativity humming.

https://arstechnica.com/tech-policy/2025/11/the-internet-archive-survived-major-copyright-losses-whats-next/

YouTube denies AI was involved with odd removals of tech tutorials



Those users could become loyal to Microsoft, White said. And eventually, some users may even “get tired of bypassing the Microsoft account requirements, or Microsoft will add a new feature that they’ll happily get the account for, and they’ll relent and start using a Microsoft account,” White suggested in his video. “At least some people will, not me.”

Microsoft declined Ars’ request to comment.

To White, it seemed possible that YouTube was leaning on AI to catch more violations but perhaps recognized the risk of over-moderation and, therefore, wasn’t allowing AI to issue strikes on his account.

But that was just a “theory” that he and other creators came up with, but couldn’t confirm, since YouTube’s chatbot that supports creators seemed to also be “suspiciously AI-driven,” seemingly auto-responding even when a “supervisor” is connected, White said in his video.

Absent more clarity from YouTube, creators who post tutorials, tech tips, and computer repair videos were spooked. Their biggest fear was that unexpected changes to automated content moderation could unexpectedly knock them off YouTube for posting videos that in tech circles seem ordinary and commonplace, White and Britec said.

“We are not even sure what we can make videos on,” White said. “Everything’s a theory right now because we don’t have anything solid from YouTube.”

YouTube recommends making the content it’s removing

White’s channel gained popularity after YouTube highlighted an early trending video that he made, showing a workaround to install Windows 11 on unsupported hardware. Following that video, his channel’s views spiked, and then he gradually built up his subscriber base to around 330,000.

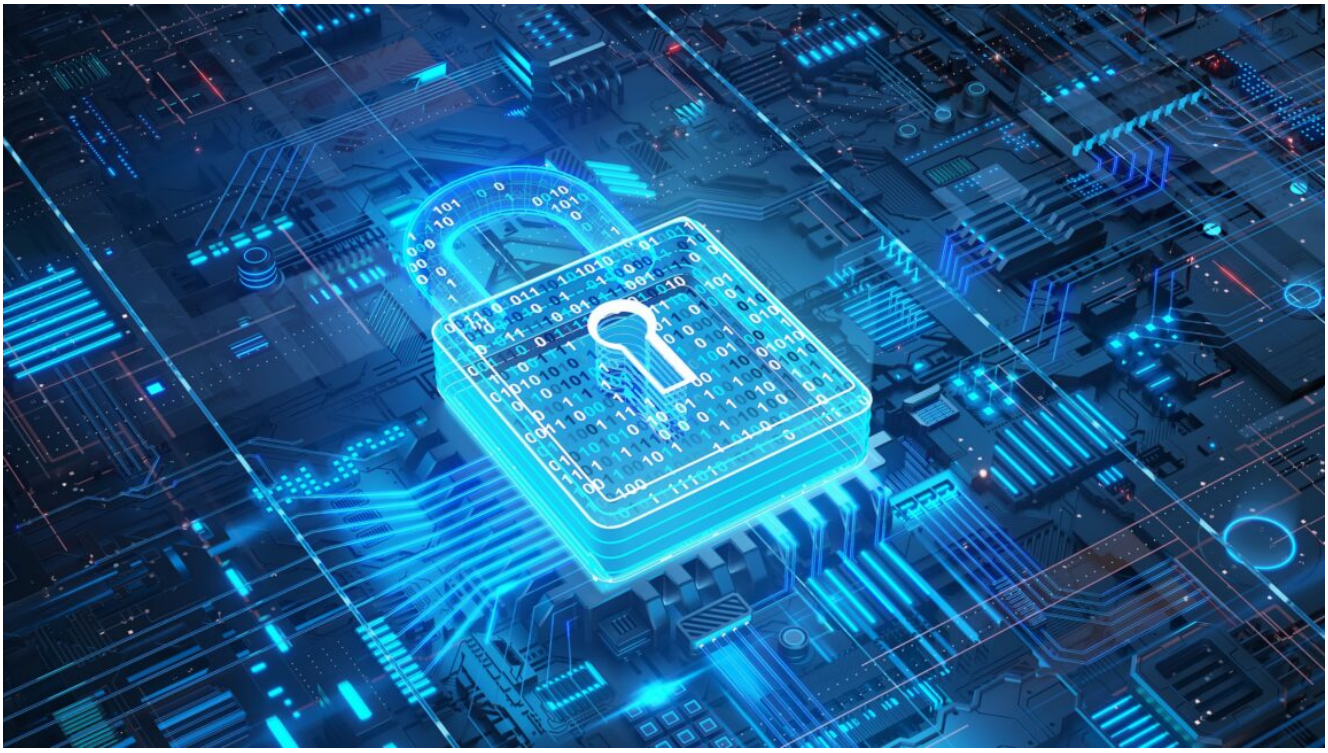
In the past, White’s videos in that category had been flagged as violative, but human review got them quickly reinstated.

“They were striked for the same reason, but at that time, I guess the AI revolution hadn’t taken over,” White said. “So it was relatively easy to talk to a real person. And by talking to a real person, they were like, ‘Yeah, this is stupid.’ And they brought the videos back.”

Now, YouTube suggests that human review is causing the removals, which likely doesn’t completely ease creators’ fears about arbitrary takedowns.

https://arstechnica.com/tech-policy/2025/10/youtube-denies-ai-was-involved-with-odd-removals-of-tech-tutorials/

FCC to rescind ruling that said ISPs are required to secure their networks



The Federal Communications Commission will vote in November to repeal a ruling that requires telecom providers to secure their networks, acting on a request from the biggest lobby groups representing Internet providers.

FCC Chairman Brendan Carr said the ruling, adopted in January just before Republicans gained majority control of the commission, “exceeded the agency’s authority and did not present an effective or agile response to the relevant cybersecurity threats.” Carr said the vote scheduled for

November 20 comes after “extensive FCC engagement with carriers” who have taken “substantial steps… to strengthen their cybersecurity defenses.”

The FCC’s January 2025 declaratory ruling came in response to attacks by China, including the Salt Typhoon infiltration of major telecom providers such as Verizon and AT&T. The Biden-era FCC found that the Communications Assistance for Law Enforcement Act (CALEA), a 1994 law, “affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications.”

“The Commission has previously found that section 105 of CALEA creates an affirmative obligation for a telecommunications carrier to avoid the risk that suppliers of untrusted equipment will ‘illegally activate interceptions or other forms of surveillance within the carrier’s switching premises without its knowledge,’” the January order said. “With this Declaratory Ruling, we clarify that telecommunications carriers’ duties under section 105 of CALEA extend not only to the equipment they choose to use in their networks, but also to how they manage their networks.”

ISPs get what they want

The declaratory ruling was paired with a Notice of Proposed Rulemaking that would have led to stricter rules requiring specific steps to secure networks against unauthorized interception. Carr voted against the decision at the time.

Although the declaratory ruling didn’t yet have specific rules to go along with it, the FCC at the time said it had some teeth. “Even absent rules adopted by the Commission, such as those proposed below, we believe that telecommunications carriers would be unlikely to satisfy their statutory obligations under section 105 without adopting certain basic cybersecurity practices for their communications systems and services,” the January order said. “For example, basic

cybersecurity hygiene practices such as implementing role-based access controls, changing default passwords, requiring minimum password strength, and adopting multifactor authentication are necessary for any sensitive computer system. Furthermore, a failure to patch known vulnerabilities or to employ best practices that are known to be necessary in response to identified exploits would appear to fall short of fulfilling this statutory obligation.”

https://arstechnica.com/tech-policy/2025/10/fcc-dumps-plan-for-telecom-security-rules-that-internet-providers-dont-like/