“Zuck off”: Doctors, nurses, scientists rail against Zuckerberg

Enlarge / Facebook CEO Mark Zuckerberg testifying before Congress in April 2018. It wasn’t his only appearance in DC this decade.

reader comments

65 with 40 posters participating

Share this story

Covid-19 Coverage

View more stories

San Francisco city officials are considering condemning the decision to name a local public hospital after Mark Zuckerberg—a move backed by nurses and doctors at the hospital, who have been railing against the Facebook co-founder and CEO since the hospital changed its name in 2015.

San Francisco Supervisor Gordon Mar on Tuesday introduced a resolution to the board of supervisors that would condemn the Zuckerberg name. The resolution also urges the city to establish clear rules on naming rights that reflect the city’s “values and a commitment to affirming and upholding human rights, dignity, and social and racial justice.”

Doctors and nurses at the hospital have been campaigning for the hospital to drop the name since it was first introduced in

2015, following a $75 million donation from Zuckerberg and his wife, Priscilla Chan, a pediatrician who used to work at the hospital. Over the years, hospital staff have expressed concern that the hospital is associated with Facebook and all of its problems and controversies—including, but not limited to, those related to privacy, unethical research, the dissemination of misinformation, hate speech, and disinformation.

They have written op-eds in local papers, signed petitions, passed out buttons reading “Zuck off,” and circulated letters. In one 2018 demonstration, nurses took a roll of blue masking tape to the large metal sign at the hospital’s main entrance, completely covering up “Zuckerberg” from the name.

Though protest has died down as health care workers struggle to address the raging COVID-19 pandemic, opposition to the name is still smoldering. Robert Brody, an internal medicine physician at the hospital, circulated an email last month asking hospital staff to consider removing “Zuckerberg” from email signatures, presentations, and research papers, according to a report by Stat. He promotes the idea with the tagline “X to the Z.”

“Whether we like it or not, Zuckerberg’s name is attached to our institution,” Dr. Brody wrote in the email. “Looking into a future desperate for institutional funding, our leaders are unlikely to support any effort to change the official name back to San Francisco General Hospital. But that doesn’t mean

we, who work here, have to use the Z name or letter.”

Naming rights

Enlarge / The Zuckerberg San Francisco General Hospital and Trauma Center sign that was partly covered during a 2018 demonstration.

In an email to Ars, the hospitals’ chief communications officer, Brent Andrew, said that the hospital is not considering changing its name. The hospital released a statement saying that “The couple’s $75 million gift in 2015 allowed the hospital to acquire state-of-the-art technology we use every single day to save patient lives, and by providing continuing support of renovations, improvements in patient care and education”

However, Andrew noted that the city’s board of supervisors is actually the body that has naming authority over the hospital. In fact, it was the board itself that approved the Zuckerberg name back in 2015.

The supervisors at the time—who are almost entirely different from the supervisors that comprise the current board—noted in its approval of the resolution:

> *It is customary and the philanthropic standard for hospitals, whether private or public in nature, to recognize major philanthropic gifts from private individuals by providing naming in honor of such gifts, whether the naming is associated with an entire hospital, hospital and health*

> *system, or a building or designated space within the institution.*

With the resolution, the board agreed to change the name from the "San Francisco General Hospital and Trauma Center" to the "Priscilla and Mark Zuckerberg San Francisco General Hospital and Trauma Center." However, in practice, the hospital almost exclusively goes by "Zuckerberg San Francisco General and Trauma Center" or just ZSFG.

The resolution also stated that the new name "shall remain in place for 50 years."

It's unclear if the board can break that agreement. Amid Facebook's Cambridge Analytica scandal in 2018, another board member—Aaron Peskin—asked the city attorney to outline a procedure for removing Zuckerberg's name from the hospital, according to the San Francisco Chronicle. The outcome of that inquiry was not released publicly. However, Andrew indicated to Ars that the board does have the power to change the name.

Ongoing fight

Meanwhile, opposition to the name continues at the hospital. Mike Dingle, a retired nursing aide who came up with the "Zuck off" slogan and buttons, suggested to Stat that he was working on "Zuck off" face masks.

And the protest from hospital staff is just one front of the opposition that Zuckerberg and Facebook are currently facing. More than 1,000 companies have stopped buying ads on the social media platform as part of a Stop Hate for Profit campaign. The campaign accuses Facebook of a "long history of allowing racist, violent, and verifiably false content to run rampant on its platform."

Separately, 260 scientists funded through the Chan Zuckerberg Initiative (CZI) or the CZ Biohub wrote an open letter to

Zuckerberg last month urging him to improve Facebook's policies on hate speech and misinformation.

"The spread of deliberate misinformation and divisive language is directly antithetical" to the mission of CZI, they wrote, which is stated as using technology to "'help solve some of our toughest challenges—from preventing and eradicating disease, to improving learning experiences for kids, to reforming the criminal justice system' and 'to build a more inclusive, just, and healthy future for everyone.'"

https://arstechnica.com/?p=1694274

Google reportedly peeks into Android data to gain edge over third-party apps

reader comments

43 with 35 posters participating, including story author

Share this story

Google for several years has collected app-usage data collected from Android phones to develop and advance its own competing apps, a new report alleges.

The project, called Android Lockbox, "collects sensitive Android user data" for use within Google and has been in

effect since at least 2013, The Information reports.

An internal team that tracks the worldwide usage of Google's first-party apps "also has used Lockbox data on third-party apps to show executives how Google services were performing compared to rivals," sources told The Information. The data was used earlier this month in India, where Google planned to roll out a competitor app to TikTok.

The information is collected through Google Mobile Services, the collection of apps and APIs such as Google, Chrome, Gmail, Google Drive, and Google Maps that usually comes pre-installed with Android.

Google told The Information that it does access usage data on other Android developers' apps but only through an API that has also been available to third-party developers since 2014. While the API grants developers access to information about phones on which their apps are installed, however, Google has much wider insight into the broad pool of all Android phones globally.

A Google representative told The Information, "The API doesn't obtain any information about in-app activity and our collection of this data is disclosed to and controllable by users" but did not comment on how Google uses that or any other data to research or develop competitors to other apps.

Sound familiar?

If The Information's allegations are accurate, antitrust regulators are likely to have a whole lot of questions for Google.

As we here at Ars have explained before, antitrust law isn't just about monopolies. It's also about a broad bucket of behaviors that are considered *anticompetitive* under the law. Using your power as one of the biggest companies in the world

to put the squeeze on startups who could eventually become viable, serious competitors is one of those anticompetitive behaviors, and regulators don’t like it.

Four of the biggest US tech firms—Alphabet (Google), Amazon, Apple, and Facebook—are all under a bevy of state, federal, and international antitrust probes at this moment, investigating whether—and, if so, to what extent—those companies grew and maintained their market power through underhanded, unlawful tactics.

Facebook in particular has been scrutinized for using data on competitors in almost exactly the way the new report accuses Google of doing. The social giant used a VPN it acquired, called Onavo, to redirect traffic through Facebook servers, where it could be logged and analyzed. That data let Facebook see what competition apps were growing in popularity so that it could then either buy out those start-ups or launch competitors.

One of those competitors was Snapchat. Last fall, reports surfaced that Snap for several years kept a dossier, called Project Voldemort, documenting Facebook’s attempts first to acquire it and later, after acquisition didn’t work, to copy Snapchat’s key features.

US investigators are also widely assumed to be probing the way in which Apple can leverage data from the iOS App Store to inform its own software development. The EU is also probing the way Apple privileges its first-party apps after Spotify last year filed a complaint against the company.

https://arstechnica.com/?p=1694260

Trump campaign angry that cell carriers blocked spammy texts to voters

Getty Images | pagadesign

reader comments

157 with 101 posters participating

Share this story

President Trump’s re-election campaign has accused Verizon, AT&T, and T-Mobile of “suppression of political speech” over the carriers’ blocking of spam texts sent by the campaign.

The fight was described Wednesday in an in-depth article by Business Insider and other reports. “The Trump campaign has been battling this month with the biggest US cellphone carriers over an effort to blast millions of cell users with texts meant to coax them to vote or donate,” Business Insider wrote. “President Donald Trump’s adviser and son-in-law, Jared Kushner, didn’t appreciate it when AT&T, Verizon, and T-Mobile blocked mass campaign texts to voters. He called the companies to complain, setting off the legal wrangling.”

When contacted by Ars, a Trump campaign spokesperson said that “any effort by the carriers to restrict the campaign from contacting its supporters is suppression of political speech. Plain and simple.” The Trump campaign statement also said it “stands by the compliance of its texting programs” with the US Telephone Consumer Protection Act (TCPA) and Federal Communications Commission guidelines.

We asked the Trump campaign to explain exactly why the texts are legal and shouldn't have been blocked but did not get a response. The Trump campaign also did not answer our questions about how many people it tried to send the texts to and about whether the texts were unsolicited or sent to people who had signed up for campaign communications.

We also asked both the Trump campaign and carriers if they've come to any agreement on how to handle texts for the rest of this year's presidential campaign but did not get any answers.

Business Insider wrote that "the showdown got serious at the start of July when Trump's team sent a blast of texts to people who hadn't signed up for them," and "a third-party firm hired to screen such messages for the major cellphone companies blocked the texts." The article said that campaign lawyers and the carriers "are still fighting over what kinds of messages the campaign is allowed to send and what the companies have the power to stop."

Politico wrote about the dispute on Monday. "People familiar with the chain of events said Verizon, T-Mobile and AT&T flagged potential regulatory problems with the peer-to-peer messaging operation, which differs from robo-texting in that texts are sent individually, as opposed to a mass blast," Politico wrote. "But within Trump's orbit, the episode has further fueled suspicions that big tech companies are looking to influence the election."

"Hi it's Pres. Trump."

One Trump-campaign text reportedly sent this week said, "Hi it's Pres. Trump. I need your help ASAP to FIGHT BACK against the radical left & take back my majority. Take a stand NOW." Trump-campaign texts reviewed by Business Insider did not include an option to unsubscribe, the news outlet's article said.

Carriers “viewed the texts as a possible violation of federal anti-robocall laws and Federal Communications Commission rules that come with hefty fines,” Business Insider reported, citing information provided by “two Republicans familiar with the effort.”

Trump “campaign operatives” contend that its texting “exists in a legal gray area that allows campaigns to blast cellphone users if the messages are sent manually,” Business Insider also wrote. TCPA restrictions apply to messages sent with an “automatic telephone dialing system.”

The FCC says its rules “ban text messages sent to a mobile phone using an autodialer unless you previously gave consent to receive the message or the message is sent for emergency purposes,” and that customers “should be able to opt out of receiving texts.”

Business Insider said the Trump campaign also argues that a recent FCC ruling “loosened the rules on what counted as spam.” That FCC order, which is being challenged by the National Consumer Law Center and other consumer-advocacy groups, says the following:

> *By this Declaratory Ruling, we clarify that the fact that a calling platform or other equipment is used to make calls or send texts to a large volume of telephone numbers is not probative of whether that equipment constitutes an autodialer under the TCPA. Instead, we make clear that if a calling platform is not capable of originating a call or sending a text without a person actively and affirmatively manually dialing each one, that platform is not an autodialer and calls or texts made using it are not subject to the TCPA’s restrictions on calls and texts to wireless phones. We further confirm that, even when a party uses an autodialer to send a message, it may still avoid TCPA liability by obtaining the recipient’s prior express consent.*

We asked the FCC if it is investigating whether the Trump-campaign texts violated robotext and spam rules, and will update this article if we get a response.

CTIA: Senders need “prior consent”

Carriers are remaining silent publicly on the dispute with Trump’s campaign. When contacted by Ars, Verizon, AT&T, and T-Mobile all declined to give statements or answer our questions. T-Mobile told Ars there has been “inaccurate reporting” on this topic but did not say what has been inaccurately reported. Verizon and AT&T referred our questions to the CTIA mobile-industry lobby group, but CTIA declined to answer our questions about the Trump texts.

CTIA did, however, provide a general statement saying, “We expect all senders—whether airlines, schools, banks or campaigns—to include clear opt-out language and gain prior consent before sending a text. These simple steps help protect consumers from spam, and maintain text messaging as a trusted medium for everyone.”

The third-party firm that blocked the texts on behalf of the carriers is Zipwhip, according to a Republican source quoted by Business Insider. Zipwhip told Ars that it is “not able to comment on our contracts, customers or their texting traffic.”

“Zipwhip’s compliance process requires all texting traffic to follow industry-standard guidelines, including where appropriate, a requirement to obtain consent from the message recipient,” the company told Ars. “The goal of the industry standard is to protect consumers from receiving unwanted messages and spam and maintain trust in texting as a communications medium.”

CTIA last year issued a set of “Messaging Principles and Best Practices” to “clarify that organizations should obtain opt-in consent before sending text messages to consumers.”

Consumers get more unwanted political texts

Last week, CTIA posted a blog specifically about spam texts from political campaigns. “Text messaging can be a very powerful and effective way to organize, inform and engage voters, but only if used the right way,” CTIA wrote. “Billions of texts will be sent from political campaigns of both parties, and we are increasingly hearing from customers that they are getting texts they didn’t ask to receive.”

Text senders should be “communicating only with consumers who have opted in, telling consumers how to opt out—by replying ‘STOP,’ for example—honoring those opt-out requests, and establishing clear privacy and security policies and practices,” CTIA said.

https://arstechnica.com/?p=1694249

CBS’ overzealous copyright bots hit Star Trek virtual Comic-Con panel

reader comments

84 with 65 posters participating

Share this story

San Diego Comic-Con—like just about every large conference, convention, and gathering in 2020—has had to switch to an online-only virtual format this year due to the continuing pandemic. Media companies that usually have a large presence at events like SDCC worked hard to create streaming alternative content—but it seems they forgot to tell their copyright bots.

ViacomCBS kicked things off today with an hour-long panel showing off its slew of current and upcoming *Star Trek* projects: *Discovery*, *Picard*, *Lower Decks*, and *Strange New Worlds*.

The panel included the cast and producers of *Discovery* doing a read-through of the first act of the season 2 finale, "Such Sweet Sorrow, Part 2." The "enhanced" read-through included sound effects, effects shots, and storyboard images meant to bolster the actors as they delivered lines from their living rooms and home offices.

Even if the presentation didn't look like a real episode of *Discovery* to the home viewer, it apparently sounded close enough: after the *Star Trek* Universe virtual panel began viewers began to lose access to the stream. In place of the video, YouTube displayed a content ID warning reading: "Video unavailable: This video contains content from CBS CID, who has blocked it on copyright grounds."

After being blacked out for about 20 minutes, the panel was restored, and the recording of the virtual panel has no gaps in playback.

Obviously, CBS would not benefit from pulling its own marketing material offline on purpose; it seems most likely that software simply heard a match, made a match, and threw up a notice until a human could override and fix it. Unfortunately, it seems an array of media companies are each

going to have to rush to correct the error in turn: two hours later, io9 reporter Beth Elderkin tweeted that a Cartoon Network panel livestream was pulled offline due to a copyright claim from Turner, Cartoon Network's parent company.

https://arstechnica.com/?p=1694047

EU demands major concessions from Google over Fitbit deal

Valentina Palladino

reader comments

29 with 22 posters participating

Share this story

The EU has demanded that Google make major concessions relating to its $2.1 billion acquisition of fitness-tracking company Fitbit if the deal is to be allowed to proceed imminently, according to people with direct knowledge of the discussions.

Since it was announced last November, the acquisition has faced steep opposition from consumer groups and regulators, who have raised concerns over the effect of Google's access to Fitbit's health data on competition.

EU regulators now want the company to pledge that it will not use that information to "further enhance its search advantage"

and that it will grant third parties equal access to it, these people said.

The move comes days after the EU regulators suffered a major blow in Luxembourg, losing a landmark case that would have forced Apple to pay back €14.3 billion in taxes to Ireland.

Brussels insiders said that a refusal by Google to comply with the new demands would probably result in a protracted investigation, adding that such a scenario could ultimately leave the EU at a disadvantage.

“It is like a poker game,” said a person following the case closely. “In a lengthy probe, the commission risks having fewer or no pledges and still having to clear the deal.”

They added that the discussions over the acquisition were “intense,” and there was no guarantee that any agreement between Brussels and Google would be reached.

Google had previously promised it would not use Fitbit’s health data to improve its own advertising, but according to Brussels insiders, the commitment was not sufficient to assuage the EU’s concerns nor those of US regulators also examining the deal.

Earlier this month, Brussels sent out questionnaires to rivals to assess whether the transaction has the potential to damage competition and disadvantage other fitness tracking apps in Google’s Play Store.

A number of consumer groups, including Europe’s umbrella consumer organization BEUC and the Consumer Federation of America, have strongly warned against the deal.

Separately, the Australian Competition and Consumer Commission also raised concerns that the transaction could help strengthen Google’s position.

Google declined to comment on the specifics of its latest

discussions with the European Commission but pointed to an earlier statement saying, “Throughout this process we have been clear about our commitment not to use Fitbit health and wellness data for Google ads and our responsibility to provide people with choice and control with their data.

“Similar to our other products, with wearables, we will be transparent about the data we collect and why. And we do not sell personal information to anyone.”

The European Commission, which has until August 8 to make a decision on the deal, declined to comment.

https://arstechnica.com/?p=1694008

Woz sues YouTube over “bitcoin giveaway” scam videos using his name

Enlarge / A screenshot from Wozniak’s lawsuit shows a typical “Bitcoin giveaway” scam video on YouTube.
YouTube / Wozniak et al

reader comments

65 with 49 posters participating, including story author

Share this story

Apple co-founder Steve Wozniak has sued YouTube over the proliferation of “bitcoin giveaway” scam videos on the YouTube

platform. The videos falsely use the names of Wozniak and other celebrities—including Elon Musk, Bill Gates, and Ethereum founder Vitalik Buterin—to give the scams legitimacy.

Scammers hijack popular YouTube accounts and change their names so that they appear to be the official accounts of celebrities like Wozniak or companies like Apple. They then broadcast a "live" video showing old footage of the celebrity discussing cryptocurrency or related topics. Alongside the footage is text claiming that if someone sends bitcoin to a particular address, the celebrity would send back double the amount.

Along with Wozniak, the plaintiffs include more than a dozen individuals who were taken in by the scam, losing bitcoins worth anywhere from a few dollars to more than $40,000. In total, cryptocurrency scams like this have cost victims millions of dollars.

"We take abuse of our platform seriously, and take action quickly when we detect violations of our policies, such as scams or impersonation," a YouTube spokesperson told Ars by email. YouTube says that in the first quarter of 2020, the company removed 2.2 million videos and disabled 1.7 million accounts for "spam, scams, deceptive practices."

But the plaintiffs argue that YouTube isn't doing nearly enough to stamp out these cryptocurrency scams. Wozniak's wife, Janet, says that she has contacted YouTube numerous times since May about the scams. The plaintiffs point out that YouTube has sophisticated tools for identifying objectionable activity. Yet they don't seem to be taking even obvious steps like filtering out videos that use terms like "bitcoin giveaway."

The lawsuit also points to the example of Twitter, which had been plagued by these kinds of scams in the past but has taken steps to stamp them out in recent years. The plaintiffs argue

that the Twitter crackdown pushed scammers to YouTube, where they have thrived for the last couple of years.

YouTube has a powerful defense

Ultimately, it may not matter how much YouTube has done to stamp out these videos. That's because Section 230 of the Communications Decency Act provides online platforms with broad immunity for user-submitted content. Sites have immunity even if they do little or nothing to combat objectionable content posted by users.

Anticipating this defense, the plaintiffs try to distinguish their lawsuit from run-of-the-mill Section 230 cases. But it's not obvious those arguments will be successful. For example, Woz's lawyers argue that the scam videos are "blatant criminal conduct that is not even arguably protected by the First Amendment." That might be true, but it isn't likely to save the lawsuit. After all, the courts have upheld Section 230 immunity even in cases where users were distributing child pornography.

The plaintiffs argue that YouTube did more than passively host the videos. YouTube's recommendation algorithms promoted the videos to cryptocurrency enthusiasts and sold ads against the videos—directly profiting from the scams. But that could also be a hard sell; courts have repeatedly held that sites enjoy Section 230 protections even when they deliberately promote problematic third-party content.

But while Woz's lawsuit is on shaky ground legally, it could still be significant in the court of public opinion. Being sued by one of Silicon Valley's most beloved figures could pressure YouTube into taking the problem of cryptocurrency scams more seriously.

https://arstechnica.com/?p=1693857

US Navy’s next warship will have an Italian accent

reader comments

14 with 13 posters participating

Share this story

Video transcript still processing but will be available soon.
The search for a replacement for the US Navy’s “little crappy ship” is over. On April 30, the US Navy announced that Fincantieri Marinette Marine, the US shipyard subsidiary of Italian shipbuilder Fincantieri, had beaten out the rest of the field to take on the FFG(X) frigate program, the shipbuilding effort that will replace the Navy’s Littoral Combat Ship (LCS).

Frigates were once the workhorses of the Navy—small, fast escort ships that hunted submarines, acted as part of the air defense ring around carriers and other big combatants, and could patrol the seas on their own when necessary. The Oliver Hazard Perry (FFG-7) class of frigates, the first US Navy ships with gas turbine engines, were worked far beyond expectations during their service; they survived attacks by errant Iraqi anti-ship missiles (in the case of the USS *Stark*) and Iranian sea mines (the USS *Samuel B. Roberts*) during the US Navy’s confrontation with Iran in the 1980s.

They were replaced by the LCS—a ship that was supposedly

designed for multiple missions and the sort of close-ashore fighting that looked like the future in the late 1990s and early days of the Global War on Terror. But that didn't turn out too well.

Fiat of the sea

Fincantieri is well-known in the commercial shipbuilding world. It has built mega-yachts and cruise ships (including Disney Cruise Lines' *Magic*) along with more than 50 naval ships in the past 20 years. Marinette Marine has long been building boats and small ships for the US Navy and Coast Guard. Before partnering with Lockheed Martin to build the LCS class, the Wisconsin shipyard built minesweepers, fleet tugs, patrol craft and other workhorse craft.

The winning design is based on the FREMM ("Fregata europea multi-missione") frigate, already in service with the Italian and French navies. A total of 20 frigates will be delivered if the contract runs its course; the first ship will cost about $1.3 billion, with the price for future ships dropping to below $950 million.

The FFG(X) will differ from the French and Italian FREMMs in a few meaningful ways. They'll be fitted with sensor and weapons systems provided as off-the-shelf "government furnished equipment"—including COMBATSS-21, a combat management system built using the Aegis program's common source library of software, and Raytheon's AN/SPY-6 radar (designed for the third flight of Arleigh Burke(DDG-51) class guided missile destroyers. And they'll be built, at least at first, entirely at a shipyard in Wisconsin that has previously partnered with Lockheed Martin to build the now-unloved Freedom LCS class.

But when the competition began to build a new frigate for the US Navy, Fincantieri was considered a long shot by most analysts. The company was up against LCS incumbents Lockheed Martin and Austal, defense contracting heavyweight General

Dynamics, and US' largest defense shipbuilder, Huntington-Ingalls (builders of the DDG-51 destroyers).

In hindsight, it seems obvious that the "advantages" the other companies had are exactly why Fincantieri Marinette won. Stung by the cost overruns on other recent combat ships, the Navy crafted the FFG X competition to reduce risk, favoring proven designs. Of the designs presented, Fincantieri's is the most proven: 19 FREMM frigates are already afloat, 10 of them built by Fincantieri.

The other designs may have been seen as too risky. Huntington-Ingalls proposed a radical redesign of the US Coast Guard's Legend-class National Security Cutter, which the Navy may have seen as too risky. General Dynamics' Bath Iron Works, which is building the very expensive Zumwalt class destroyers, pitched a ship based on Spain's cancelled F100 design. And Lockheed Martin and Austal had pitched up-sized versions of their LCS designs—designs that may have been seen as more of a liability (Lockheed dropped out of the hunt early, despite being seen as a favorite).

Bloated "Streetfighters," begone

The LCS was the product of a late 1990s concept for small, inexpensive but heavily armed ships that could operate in shallow waters close to enemies' coasts, dubbed "Streetfighter." But the LCS concept evolved under President Bush's administration into a larger ship that could accept swappable mission modules for tasks such as antisubmarine warfare, mine warfare, and combatting small armed boats.

What the Navy ended up getting instead, after long delays, was a pair of ship designs that cost more to operate than the frigates they replaced. They could not easily swap mission modules, they had totally different sensor systems than other ships, they were more vulnerable to air attack, and they had less "survivability" than the Perry class.

While the LCS ships got bigger, their crews (and damage control capabilities) remained small, and their designs remained suited to taking on only low-intensity missions. By contrast (as if the survival of the *Stark* and *Roberts* wasn't enough evidence of the Perry class' superior ability to take punishment), the decommissioned Perry class frigate ex-USS *Thatch* was hit during a 2016 exercise with two Harpoon missiles, two hellfire missiles, a Maverick missile, two bombs, and a Mark 48 torpedo—and still took 12 hours to sink.

China's growing Navy and posture in the South China Sea, as well as other growing threats from "peer" powers and some angry words from Congress, eventually convinced the Navy that a more capable ship than the LCS was needed—and that it had to be one they could get quickly and inexpensively. At one point, the Navy considered bringing Perry class frigates out of mothballs because of the gaps in capabilities left by the LCS' shortcomings.

The FFG(x) won't arrive overnight. The first ship should be delivered in 2026 if all goes according to plan. But if it lives up to its design intentions, it may be the first ship in the last 20 years that delivers what the Navy has paid for.

Listing image by MediaNews Group/Long Beach Press-Telegram via Getty Images

https://arstechnica.com/?p=1683795

QAnon conspiracy kicked off

Twitter as platform bans thousands of accounts

Enlarge / A cluster of Trump supporters, sporting Q-emblazoned T-shirts and the campaign's signature red MAGA hats, waiting in line to get into a rally in Tennessee in 2018.

reader comments

87 with 46 posters participating

Share this story

Twitter is removing thousands of accounts and tweets that support the baseless QAnon conspiracy theory from its platform, citing the movement as "coordinated harmful activity" that leads to harassment and other harms.

"We've been clear that we will take strong enforcement action on behavior that has the potential to lead to offline harm," the company announced in—naturally—a series of tweets. "In line with this approach, this week we are taking further action on so-called 'QAnon' activity across the service."

In addition to suspending more than 7,000 accounts so far—and possibly as many as 150,000 before all is said and done—Twitter says it will no longer include anything associated with QAnon in trends or recommendations, make sure not to highlight it in search, and block certain URLs associated with Q from Twitter.

Q-related content has apparently been on the upswing lately, which is perhaps not surprising, as the US is currently experiencing both an out-of-control pandemic and a widespread civil rights protest movement at the same time. Adherents have

also apparently been trying to do end-runs around Twitter's rules, which the platform is also pushing back on. "We will permanently suspend accounts Tweeting about these topics that we know are engaged in violations of our multi-account policy, coordinating abuse around individual victims, or are attempting to evade a previous suspension—something we've seen more of in recent weeks," Twitter wrote.

The FBI last year warned that QAnon and other "anti-government, identity-based, and fringe political conspiracy theories" posed a concrete threat to domestic safety.

"Although conspiracy theory-driven crime and violence is not a new phenomenon," the FBI wrote at the time, "today's information environment has changed the way conspiracy theories develop, spread, and evolve."

The agency also specifically warned of continuing threats as the 2020 election approaches, writing that domestic fringe movements, "very likely will emerge, spread, and evolve in the modern information marketplace over the near term, fostering anti-government sentiment, promoting racial and religious prejudice, increasing political tensions, and occasionally driving both groups and individuals to commit criminal or violent acts."

To date, QAnon followers have been tied to at least a half-dozen violent incidents, including kidnappings, attempted arson, and at least one murder.

"It's a letter of the alphabet, as far as I know…"

Three years ago, QAnon kicked off with an anonymous post on 4chan claiming to have insider information about former secretary of state and recent presidential candidate Hillary Clinton and grew from there. As with many conspiracy theories,

the details are somewhat inchoate and often contradictory, but the core belief more or less posits that an anonymous insider (or insiders) known as “Q” is sharing information about President Donald Trump’s tortuous, long-term plans to take down the “deep state.”

QAnon has since oozed from the Internet’s most unsavory corners into the right-wing mainstream, picking up celebrity endorsements along the way. Trump has amplified QAnon-related messages on Twitter, and signs from Q adherents are a regular appearance at his in-person rallies. At least eight QAnon supporters have a chance at being voted into Congress this fall after winning Republican primaries in their states this spring and summer.

Making the leap from 4chan to the more accessible Reddit in 2017 and 2018 helped the Q conspiracy gain steam. Reddit ended up banning several Q-related subreddits in 2018, saying they violated site content policies. “We are very clear in our site terms of service that posting content that incites violence, disseminates personal information, or harasses will get users and communities banned from Reddit,” a spokesperson said at the time.

Facebook removed a small handful of Q-related pages in May, citing its policies against coordinated inauthentic behavior.

https://arstechnica.com/?p=1693381

DOJ: Chinese hackers stole

“hundreds of millions of dollars” of secrets

Enlarge / The Department of Justice seal as seen during a press conference in December 2019.

reader comments

131 with 77 posters participating

Share this story

Two state-sponsored hackers in China targeted US businesses in a “sophisticated and prolific threat” for more than 10 years, both for financial gain and to steal trade secrets, the Department of Justice said today.

The 11-count indictment (PDF), which was made public today, alleges Li Xiaoyu and Dong Jiazhi worked with China’s Ministry of State Security (MSS) and other agencies to hack into “hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad.”

Li and Dong were allegedly infiltrating networks of businesses in a wide array of sectors, including “high tech manufacturing; civil, industrial, and medical device engineering; business, educational, and gaming software development; solar energy; and pharmaceuticals,” as well as defense contractors, since at least September 2009. In recent months, prosecutors allege, the two were seeking ways in to “the networks of biotech and other firms publicly known for work on COVID-19 vaccines, treatments, and testing technology”

in at least 11 countries, including the US.

The indictment does not name the firms in question, only saying that "on or about January 25 and 27," Li was trying to break into networks at a Maryland biotech firm and a Massachusetts biotech firm, both of which were publicly known by that point to be working on COVID-19 vaccines. Matching up the timelines, the targets seem to have been Novavax, based in Gaithersburg, Maryland, and Moderna, based in Cambridge, Massachusetts.

In addition to several instances when the pair were allegedly working with MSS and other government entities, Li and Dong were also trying to make some money on the side, the indictment alleges. "At least once, they returned to a victim from which they had stolen valuable source code to attempt an extortion—threatening to publish on the internet, and thereby destroy the value of, the victim's intellectual property unless a ransom was paid."

Assistant Attorney General for National Security John C. Demers said in a written statement:

> *China has now taken its place, alongside Russia, Iran, and North Korea, in that shameful club of nations that provide a safe haven for cyber criminals in exchange for those criminals being "on call" to work for the benefit of the state, here to feed the Chinese Communist party's insatiable hunger for American and other non-Chinese companies' hard-earned intellectual property, including COVID-19 research.*

Russia, too, stands accused of trying to steal COVID-19-related trade secrets from other nations. On Friday, the National Security Agency and its UK and Canada counterparts said hackers linked to Russian intelligence were attempting to break into organizations that are working on potential vaccines for COVID-19. (Russia denied the allegations.)

The bigger picture

Tensions between China and the United States have been running high since 2017, particularly when it comes to technology, hacking, and national security.

This is not the first time this year the DOJ has indicted Chinese nationals for alleged high-profile hacking activity inside the US. Back in February, the DOJ said state-sponsored hackers in China were responsible for the 2017 Equifax breach, arguably the worst-ever leak of US individuals' private data.

The Trump administration is considering a ban on TikTok and other apps owned by China-based companies, Secretary of State Mike Pompeo said earlier this month. The administration is also enforcing bans on equipment made by China-based firms Huawei and ZTE, as well as sanctions preventing US companies from exports to both companies, citing national security concerns.

https://arstechnica.com/?p=1693284

Ajit Pai urges states to cap prison phone rates after he helped kill FCC caps

Enlarge / A telephone in a prison.

reader comments

95 with 71 posters participating

Share this story

Federal Communications Commission Chairman Ajit Pai is urging state governments to impose price caps on prison phone calls, three years after Pai helped kill Obama-era FCC rules that limited the price of such calls.

Pai yesterday sent a letter to the National Association of Regulatory Utility Commissioners (NARUC), saying it is up to state governments to cap intrastate calling prices because the FCC lacks authority to do so. (NARUC represents state utility regulators.) Pai wrote:

> *Given the alarming evidence of egregiously high intrastate inmate calling rates and the FCC's lack of jurisdiction here, I am calling on states to exercise their authority and, at long last, address this pressing problem. Specifically, I implore NARUC and state regulatory commissions to take action on intrastate inmate calling services rates to enable more affordable communications for the incarcerated and their families.*

Pai's letter did not mention that his own actions helped cement the status quo in which the FCC does not regulate intrastate prices. It's well-established that the FCC can regulate interstate rates, those affecting calls that cross state lines. Pai is even proposing to lower the FCC-imposed rate caps on interstate calls from 25¢ to 16¢ per minute in an order the FCC will vote on next month. But Pai's plan doesn't limit prices on intrastate calls, those in which the prisoner and the person on the other end of the line are in the same state.

Under then-Chairman Tom Wheeler, the Obama-era FCC did try to

limit intrastate prices, but those efforts were repeatedly shot down by court rulings. Shortly after President Trump appointed Pai to replace Wheeler in early 2017, Pai instructed FCC lawyers to drop the commission's court defense of a cap on intrastate calling rates. That helped lead to a June 2017 court victory for prison phone company Global Tel*Link in its lawsuit against the intrastate cap.

Pai "could've fought harder"

As Pai explains it in his proposal to further limit interstate calling rates, the FCC "has not always respected" the Communications Act's division of jurisdiction between the FCC and states. "Because the Commission has not always respected this division, the US Court of Appeals for the District of Columbia Circuit has twice remanded the agency's efforts to address rates and charges for inmate calling services," Pai's proposal says. Pai's letter yesterday said that NARUC itself "has consistently made clear its view that the FCC has no authority, and should not attempt to exercise authority, to regulate intrastate rates." NARUC has taken that position both in FCC filings and in litigation, Pai wrote.

But as UC Berkeley Law professor Tejas Narechania wrote on Twitter yesterday, the court's interpretation of US law is "an interpretation of current law [that Pai] sought, and he could've fought harder to correct."

The Wheeler-led FCC in October 2015 imposed caps on intrastate rates, arguing that it had legal authority to do so under Section 276 of the Communications Act, which says the FCC is charged with implementing Congress' directive "that all payphone service providers [be] fairly compensated for each and every completed intrastate and interstate call."

Pai voted against the October 2015 order as a member of the FCC's then-Republican minority, saying it exceeded the FCC's authority, and dropped the FCC's court defense of the order

after Republicans took the commission majority. Narechania wrote that "under Pai's leadership, the FCC decided that 'fair' meant only fair to the carrier. Not to the consumer. So while these rates were unfair to inmates, they were more than fair to the carriers."

Pai denounces "egregiously high" prices

Pai's letter to NARUC said that in the absence of FCC regulation, intrastate prices have far exceeded interstate ones:

> *FCC staff analysis has revealed that providers of inmate calling services are charging egregiously high intrastate rates across the country. Intrastate rates for debit or prepaid calls substantially exceed interstate rates in 45 states. Thirty-three states allow rates that are at least double the current federal cap, and 27 states allow excessive "first-minute" charges up to 26 times that of the first minute of an interstate call. Here are some numbers: For an interstate call, the first-minute charge may not exceed 25 cents [under FCC rules] today, but for an intrastate call, first-minute charges may range from $1.65 to $6.50. Indeed, Commission staff have identified instances in which a 15-minute intrastate debit or prepaid call costs as much as $24.80—almost seven times more than the maximum $3.15 that an interstate call of the same duration would cost.*

According to Pai's letter, this is "unfortunately a problem the FCC is powerless to address" but "state commissions around the country… can do something about it." Pai wrote that about 80 percent of inmate calls are intrastate and that "the burden of egregious rates for intrastate inmate calling services does not fall equally on everyone" because "African-Americans are disproportionately represented among the incarcerated. They

and their families are thus disproportionately reliant on inmate calling services. Yet they and their families tend to have lower incomes, making them particularly vulnerable to these exorbitant intrastate rates."

Pai wrote that NARUC has made statements condemning discrimination but that the state governments NARUC represents haven't taken enough action to limit prison phone prices. "These are noble *sentiments*. But it is time for these sentiments to manifest in *action*," Pai wrote.

We contacted NARUC about Pai's letter today and will update this article if we get a response.

https://arstechnica.com/?p=1693248