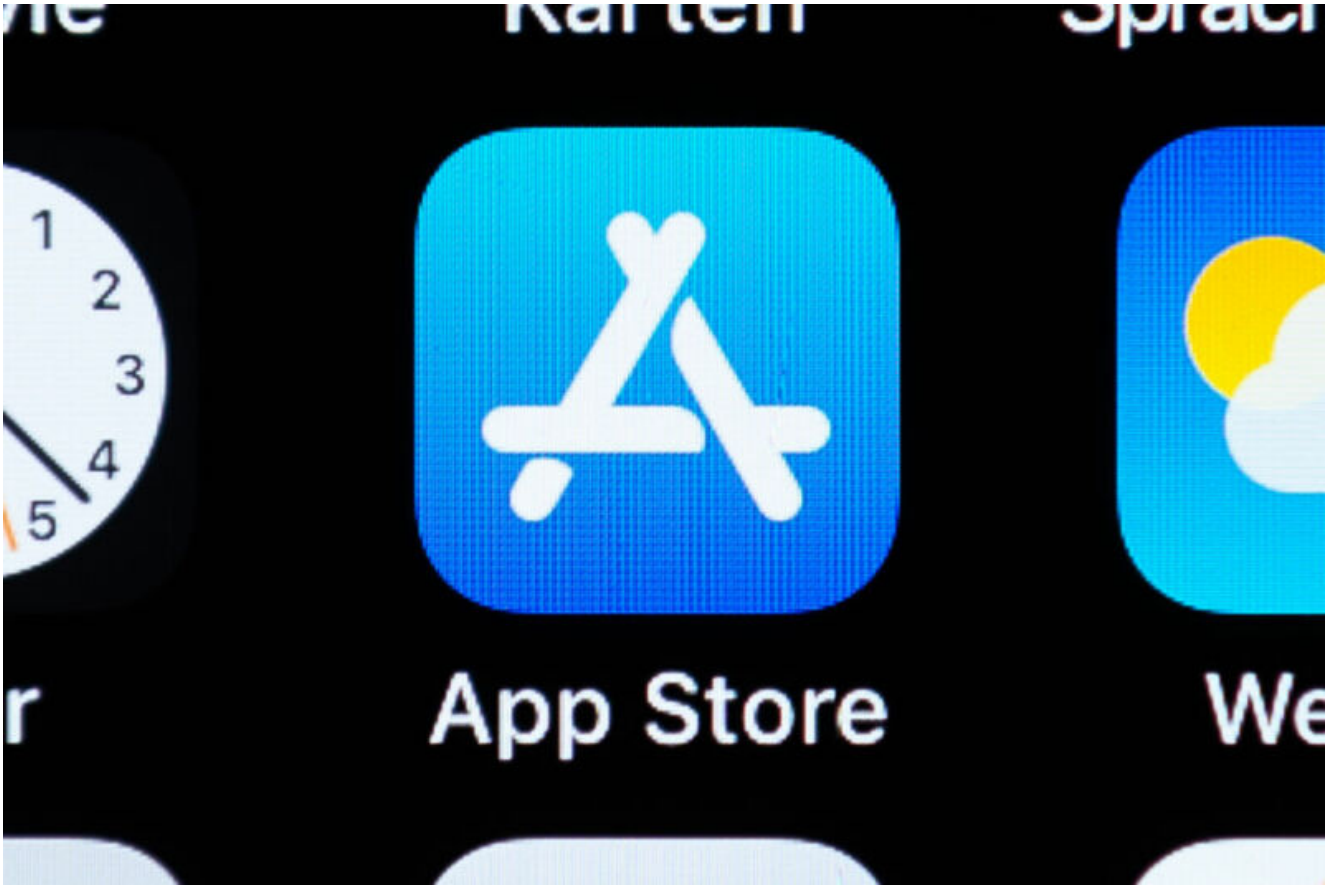
EC opens antitrust probe into Apple Pay, Apple’s App Store



Enlarge / 08 January 2019, Hessen, Rüsselsheim: ILLUSTRATION – The App Store (M) logo can be seen on the screen of an iPhone. Photo: Silas Stein/dpa (Photo by Silas Stein/picture alliance via Getty Images)

reader comments

88 with 37 posters participating

Share this story

The European Commission has opened two formal antitrust investigations into Apple’s App Store and its Apple Pay payment system.

The investigation into the App Store comes after a complaint from Spotify in March 2019 and a subsequent complaint from e-

reader company Kobo over how Apple takes a 30 percent commission on every subscription signed up through its App Store in the first year, and then a 15 percent cut.

At the same time, the companies complained, Apple has promoted its own music and books services. The European Commission is also looking at whether App Store rules stifle competition in gaming and cloud services, according to people with direct knowledge of the situation.

Apple's global App Store fees are estimated to generate more than $1 billion for the company every month. Apple said in January that consumer spending on the App Store hit a new single-day record of $386m on January 1—likely generating $50 million to $100 million for Apple itself.

The EU said that, following a preliminary investigation, "the commission has concerns that Apple's restrictions may distort competition for music streaming services on Apple's devices."

It added that by forcing companies to sell to customers through Apple's own in-app payments system, Apple seemed to have "full control over the relationship with customers of its competitors."

The commission said that Apple appeared to cut off its rivals from data about their customers and was able to obtain "valuable data about the activities and offers of its competitors."

"Apple sets the rules for the distribution of apps to users of iPhones and iPads. It appears that Apple obtained a 'gatekeeper' role when it comes to the distribution of apps and content to users of Apple's popular devices," said Margrethe Vestager, the EU's competition chief.

The EU could theoretically impose a maximum penalty of 10 percent of Apple's global revenues for breaching competition rules, but rivals suggested they were more interested in other

remedies.

“It has been shown in other fines against Google, for example, that these are merely the cost of doing business and have no meaningful impact in changing long-term business practices. Fines are not in the interest of Apple rivals or consumers,” said one adviser to an Apple rival.

In the EU, App Store users spent $3.4 billion in 2019, or $4.8 billion including the UK, according to Sensor Tower data. Apple’s digital revenues in the region are far behind China, the US and Japan, which saw $16.4 billion, $15.4 billion, and $10.2 billion of sales, respectively.

Separately, the EU is launching an investigation into Apple Pay and whether it undermines competition by limiting access to near-field communication for contactless payment in stores.

Ms. Vestager added, “It appears that Apple sets the conditions on how Apple Pay should be used in merchants’ apps and websites. It also reserves the ‘tap and go’ functionality of iPhones to Apple Pay.

“It is important that Apple’s measures do not deny consumers the benefits of new payment technologies, including better choice, quality, innovation, and competitive prices.”

Apple said the company followed the law and embraced competition. It added, “It’s disappointing the European Commission is advancing baseless complaints from a handful of companies who simply want a free ride and don’t want to play by the same rules as everyone else.”

In the past, the company has defended its fees by saying that its businesses are free not to sell through the App Store but that the platform allows access to billions of users.

Apps that pay the 30 percent commission are able to sell directly to consumers and to charge upfront for downloads.

Strong momentum in Apple's services business has become increasingly important to the company in recent years, especially as iPhone sales have fluctuated. At about 18 percent of Apple's annual sales, services are its second-largest source of income after the iPhone.

Overall services revenues grew 16 percent last year to $46.3 billion, including App Store commissions, its own music and video services, iCloud and AppleCare extended warranties.

As well as growing more rapidly than most of its hardware products, these services are much more profitable, with gross margins increasing from 55 percent in 2017 to 64 percent last year—a total of $29.5 billion—compared with 32 percent for devices.

Analysts at Morgan Stanley estimated in a research note this month that App Store net revenues had consistently exceeded $1 billion a month in recent years, likely reaching $5.2 billion for the quarter ending in June.

They predict that App Store growth will have accelerated during the coronavirus lockdowns, as consumers spend more on digital entertainment while stuck at home. Apple will hold its annual event for app developers next week, with Monday's online keynote expected to show off improvements to iOS and new Mac computers.

Apple has been under intense scrutiny in Brussels in recent weeks. Last month, tracking-app maker Tile argued in a letter sent to the commission that Apple was abusing its power to unfairly favor one of its own products.

© 2020 The Financial Times Ltd. All rights reserved. Not to be redistributed, copied, or modified in any way.

https://arstechnica.com/?p=1684120

Georgia shows why November’s election could be chaos



Enlarge / People wait to vote in Georgia’s primary election on June 9 in Atlanta.

reader comments

104 with 65 posters participating

Share this story

There’s broad agreement that last week’s primary election in Georgia was a fiasco, with voters reportedly waiting as long as five hours to cast a ballot.

Democrats accused Georgia Republican Secretary of State Brad

Raffensperger of bungling the statewide rollout of new election technology. Some went further, suggesting that the problems—which were most severe in Democratic areas—were a deliberate Republican strategy.

“What happened in Georgia yesterday was by design,” former presidential candidate Hillary Clinton tweeted last Wednesday. “Voter suppression is a threat to our democracy.”

Republicans have responded by blaming officials in Democratic-leaning urban counties where the problems were the worst. County officials in Georgia are responsible for many day-to-day details of an election, including selecting polling places and recruiting poll workers.

Raffensperger singled out officials in Fulton and DeKalb Counties—liberal jurisdictions in the heart of the Atlanta metro area. “Every other county faced these same issues and were significantly better prepared to respond so that voters had every opportunity to vote,” Raffensperger wrote in an election-day statement.

“Plenty of blame to go around”

Experts told Ars that the biggest factor wasn’t Republican or Democratic mismanagement—it was the coronavirus. The virus forced Georgia to delay its primary from March to June. Due to coronavirus fears, some counties had difficulty finding new locations for their election precincts, forcing them to combine multiple precincts in one location.

“Fulton County had a massive no-show rate on poll workers,” said Andy Green, a voting security expert at Kennesaw State University in Georgia. “There was plenty of blame to go around to all parties.

“These are new systems, we had fewer poll workers, we had fewer precincts, and we had fewer voting systems within those

precincts," Green said. "I think that if you were to ask me which one was the No. 1 cause of problems, I wouldn't be able to answer that."

But one other factor that played a significant role was a new voting system that was used for the first time statewide last week. That system included a new electronic poll book system for checking voters in as well as new ballot-marking machines. Voters had problems with both systems last week—though it's not clear if these were primarily problems with the systems themselves or that poll workers had inadequate training on how to use them.

A preview for November?

It's worth paying attention to what happened in Georgia because almost every state could face similar challenges in November. If the coronavirus is still a significant problem on November 3—which it very well could be—states may struggle to find suitable polling places and recruit enough poll workers. Many more voters are likely to vote by mail, forcing states to rapidly expand their infrastructure for counting mail-in ballots. And there's a risk foreign governments will be looking for ways to interfere.

"It's probably going to be one of the most chaotic elections in our nation's history," said Matthew Bernhard, an election security researcher at the University of Michigan, in an interview last Friday.

Election officials have a ton of work to do in order to be prepared for this November's election, experts told Ars. They need to make sure there are enough polling locations and poll workers despite concerns about the coronavirus. And most states need to build infrastructure to process an order of magnitude more mail-in ballots than they received in past elections.

Congress could help out here. Congress allocated $400 million to help states with coronavirus-related election challenges in March, but experts at the time said that a lot more was needed.

Technology played a big role in last week's voting problems

In a bid to make voting more convenient, a number of states have expanded early voting centers. These locations are typically open for several weeks before the election. Voters can visit these centers at their convenience, and they don't necessarily have to visit the one nearest their home.

Of course, this flexibility for voters creates logistical challenges for election officials. Officials need to make sure that each voter casts only one ballot and that the voter gets the right ballot based on his or her specific place of residence. Georgia, which is at the forefront of this trend, makes heavy use of technology to help manage this complexity. In last week's election, the state used Internet-based poll-book software to verify voter identities and check them in electronically. Voters were then sent to a ballot-marking device with a smart card indicating which ballot the voter should receive.

David Becker, an election expert at the Center for Election Innovation & Research, argues that digital systems are key to enabling the use of early voting centers.

"Fulton County probably has hundreds of ballot styles, based on where you live and who you're allowed to vote for," Becker told Ars last week. Without ballot-marking devices, "they would have had hundreds of stacks at each one of these polling places."

Previously, Georgia used touchscreen voting machines that

counted votes electronically—without producing a paper ballot. These machines offered convenience and flexibility, but security experts warned that the lack of a paper trail made it impossible to verify results. Last year, after a lengthy legal battle, the state promised to abandon these purely electronic voting machines in favor of ballot-marking devices—new touchscreen machines that produced a voter-readable paper ballot.

Georgia piloted its new election technology—both new ballot-marking devices and new electronic poll books—in a few local elections last November. Four of the six participating counties reported problems with the state's electronic poll-book software that tells election workers which ballot a voter should receive. The problems delayed voters by as much as 45 minutes.

The statewide rollout of the software was apparently even worse, with technology problems playing a major role.

There were problems with both voting machines and training

At one Southwest Atlanta precinct, voters faced multi-hour delays due to technology problems. According to one voter who talked to the Atlanta Journal-Courier, "in the morning a poll worker informed the crowd that all but one voting machine was down." By lunch time, the line "stretched outside the door, down the sidewalk and nearly to the road."

Fulton County Commissioner Liz Hausmann said she had to wait two and a half hours to vote, and she said several factors contributed to the delays. She told the AJC that "equipment came late, some wasn't charged and workers checking voters in weren't clear about their instructions."

But Becker, an advocate for the use of technology in

elections, argues that the problems with voting technology were overstated.

“Ten voting machines out of more than 30,000 had to be replaced statewide,” Becker told Ars. “That’s an incredibly low number.”

Becker argued that a lack of poll-worker training was a bigger issue.

“The problems with the technology were related to poll workers not having adequate training to set up and use the technology easily,” he said. Due to the coronavirus, the training was conducted virtually, so many poll workers were encountering the physical equipment for the first time on election day.

Voting security expert Harri Hursti visited Georgia last Tuesday. He agrees that a lack of training was a big issue. “They didn’t have training materials,” he told Ars. “Things that should have come from the state to the counties was missing.”

https://arstechnica.com/?p=1683650

Trump hasn’t followed through on plan to withdraw US from WHO



Enlarge / World Health Organization Director-General Tedros Adhanom Ghebreyesus at a press conference on COVID-19 at WHO headquarters in Geneva on March 11, 2020.
Getty Images | Fabrice Coffrini

reader comments

141 with 89 posters participating

Share this story

On May 29, President Trump said his administration would take immediate action to withdraw the US from the World Health Organization.

“Because they have failed to make the requested and greatly needed reforms, we will be today terminating our relationship with the World Health Organization, and redirecting those funds to other worldwide and deserving, urgent global public health needs,” Trump said at the time, while criticizing the WHO’s response to the coronavirus pandemic and claiming that “China has total control” over the United Nations agency.

But now, two weeks later, there's nothing to indicate that Trump has followed through on his plan. In an article yesterday titled "US hasn't taken action to withdraw from WHO despite Trump pledge," The Hill wrote that "no steps toward a formal withdrawal have been taken," and that "a WHO spokesman told The Hill that the agency had received no formal notification that the United States would withdraw."

Another article yesterday in Stat, a health news website, said that "none of the levers that would need to be pulled to follow through on [Trump's WHO] decision has been pulled." For example, the Trump administration has "not paid outstanding financial obligations to the WHO, a step that would be required before the United States could pull out under a joint resolution signed by Congress," the article said.

"The US is not out of WHO"

These reports follow a Vanity Fair article published Monday that describes "the secret plan to unwithdraw from the WHO after Trump's 'bizarre,' 'ruinous' exit."

Trump's WHO announcement "blindsided top federal officials," who had been working "to salvage America's relationship with the WHO" after Trump's April decision to temporarily halt US funding and his criticism of the WHO in mid-May, Vanity Fair wrote. The article continued:

> *Now, Vanity Fair has learned, secret negotiations aimed at reversing Trump's decision have begun between [US] Ambassador [Andrew] Bremberg and the WHO's director general, Dr. Tedros Adhanom Ghebreyesus. A phone call Saturday between the two men resulted in a possible framework agreement to restore the relationship, which the US diplomatic corps views as essential to the global fight against coronavirus and myriad other public health issues.*
>
> *The framework would allow for both increased scrutiny of*

> *China's conduct and an independent review of the WHO's performance in the first six months of the outbreak. And discussions continue over whether the WHO would exert pressure on China to turn over original samples of the live virus and allow its scientists to be interviewed regarding the virus's origins. "It's fair to say the US is not out of WHO, and negotiations are ongoing to address concerns and hopefully walk back from this decision," said an official who participated in a call with G7 partners, an alliance of countries with advanced economies, where this information was shared.*

The US generally provides about 15 percent of the WHO's budget and gave the organization $893 million during the WHO's two-year funding cycle that ended on December 31.

The Trump administration could still try to follow through on Trump's announced plan. But Trump's statement on May 29 was false insofar as he said the US would be "terminating our relationship" on that very day.

"Some question whether the president has the legal authority to pull the country out of the WHO—whose own constitution includes no mechanism for withdrawal by a member state," Stat wrote. "Others argue that the only way the US can withdraw was prescribed in the joint resolution of Congress that passed in 1948, meaning the US would have to file a formal notice of its intention to leave and pay its outstanding financial obligations."

A Health and Human Services (HHS) spokesperson said the US "will not be contributing funding to WHO but is happy to provide technical expertise or guidance to help end [the current Ebola] outbreak," according to Stat. A State Department spokesperson "reiterated the president's complaints against the agency and his intention to withdraw," Stat also wrote.

US and WHO had “good discussion” on Ebola

There were seemingly conflicting statements at a press conference on Wednesday about whether the US continues to support the WHO financially.

“We had a very good discussion with [HHS] secretary [Alex] Azar last week and he assured me of US’ continued commitment to support in the fight, especially against Ebola,” the WHO’s Dr. Tedros said. But later in the same press conference, Tedros clarified that he “didn’t say” whether the WHO is “receiving funding directly from the US” for the fight against Ebola in the Democratic Republic of the Congo.

“I said it many times, I think in our relationship with the US, it’s not about the money,” Tedros said. “You know, working together, the relationship, I think, is more important, and [I] hope we will work side by side to control or contain the outbreak in western DRC as soon as possible, but the cooperation doesn’t involve the financing part directly to WHO.”

Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, expressed his support for a continued US/WHO partnership yesterday. “I would hope that we could continue to benefit from what the WHO can do at the same time that they continue to improve themselves,” Fauci told CBC News. “I’ve had good relationships with the WHO and the world needs the WHO.”

https://arstechnica.com/?p=1683556

New Google rule bans discriminatory targeting for housing ads



Enlarge / A sign on the street is visible to anyone who walks or drives by. A sign online can be strategically, and illegally, targeted away from people against whom you may have a bias.

reader comments

63 with 41 posters participating

Share this story

Google is taking action to reduce unlawful discrimination on its advertising platform a year after the federal government sued its largest competitor, Facebook, over the same thing.

The company is “introducing a new personalized advertising policy for certain types of ads,” a Google executive shared in a company blog post today. The policy prohibits entities placing ads for employment, housing, or credit services from targeting *or* excluding ads “based on gender, age, parental status, marital status, or ZIP Code.”

The federal Fair Housing Act explicitly prohibits landlords and sellers from discriminating against potential renters or buyers on the basis of race, color, national origin, religion, sex, familial status, or disability. (“Family status” includes a ban on discriminating against someone who is pregnant or families with children.) That applies to the advertising of units as well as who actually gets to sign the lease or the mortgage and what they have to pay.

Google already prohibits personalization based explicitly on “race, religion, ethnicity, sexual orientation, national origin, or disability,” the post explains. Some of today’s new additions to the list, such as marital or parental status, are already protected categories. Others, such as ZIP code, can all too easily be used as proxies for other categories, such as race or ethnicity, as many existing neighborhoods are highly segregated.

This is not a new problem, and Google—which dominates the online advertising market—is not alone. A ProPublica report in 2016 found that Facebook’s system allowed for the placement of housing ads to groups that explicitly excluded certain “ethnic affinities.” A group of users sued Facebook shortly after, alleging that the site was violating federal law. Facebook promised to do better, but a full year later, in 2017, ProPublica was still able to place explicitly discriminatory rental ads, despite updated Facebook policies theoretically prohibiting the practice.

In 2019, the Department of Housing and Urban Development took legal action, alleging Facebook was acting in violation of the

Fair Housing Act by “encouraging, enabling, and causing housing discrimination through the company’s advertising platform.”

Google said in its update that it has been “working closely” with HUD on these changes. “As part of our effort, we’ll provide housing advertisers with additional information about fair housing to help ensure they are acting in ways that support access to housing opportunities,” Google added.

HUD Secretary Ben Carson also issued a statement about the new Google policy. “Advertising practices may continue to evolve, but our nation’s laws are unwavering,” Carson said. “It is one of our key duties at HUD to enforce the Fair Housing Act and ensure that all Americans have housing choice. Improvements are underway in the online advertising space, and HUD encourages platforms, such as Google, to take these types of steps to eliminate unlawful discrimination in advertising and seek to ensure compliance with our nation’s Fair Housing laws.”

https://arstechnica.com/?p=1683512

OpenZFS removed offensive terminology from its code



Enlarge / Replacements for outdated master/slave terminology tend to be considerably more accurate, as well as less offensive.

reader comments

332 with 150 posters participating, including story author

Share this story

On Wednesday evening, ZFS founding developer Matthew Ahrens submitted what should have been a simple, non-controversial pull request to the OpenZFS project: wherever possible without causing technical issues, the patch removed references to “slaves” and replaced them with “dependents.”

This patch in question doesn’t change the way the code functions—it simply changes variable names in a way that brings them in conformance with Linux upstream device-mapper terminology, in 48 total lines of code (42 removed and 48 added; with one comment block expanded slightly to be more descriptive).

But this being the Internet, unfortunately, outraged naysayers

descended on the pull request, and the comments were quickly closed to non-contributors. I first became aware of this as the moderator of the r/zfs subreddit where the overflow spilled once comments on the PR itself were no longer possible.

Updating terminology is technically sound

There are several valid answers to the "Why patch?" question. For those who refuse to think of anything but clarity, there is no good descriptive relationship between any technology and human slavery—and the human term far predates any engineering or technical use. Replacing "master/slave" terminology generally results in a more precise, easily discoverable technical description.

OpenZFS is not on the leading edge of this disambiguation effort. Some notable projects which have discarded and replaced master/slave terminology include the BIND DNS server, Drupal Web application framework, and Redis datastore. It is particularly telling that, although all three projects used the same original "master/slave" terms, the replacements were different. That's because the actual relationship described is different in each project, and so the most sensible replacement for the same original term is different for each project.

For the BIND DNS server, the Internet Systems Consortium replaced master/slave with primary/secondary. For Drupal, the replacement is primary/replica, and for Redis, it's leader/follower. The different replacement terms exist because the real functions are different—and the replacement for the original terminology is therefore more descriptive of what's actually happening underneath the hood.

Similar historical updates

As mentioned previously, OpenZFS is by no means the first project to update its codebase and documentation to remove references to slavery. Although complaints about master/slave terminology circulated at least as far back as the 1990s, the first large mainstream American exposure came from Los Angeles in 2003, where a black employee of the county filed a complaint concerning master/slave labels on videotape devices.

In addition to specific terminology updates in specific projects, the IETF (Internet Engineering Task Force) published a memo in 2018 acknowledging and outlining the problem and offering specific alternatives to both master/slave and blacklist/whitelist terminology.

Motivation and context

While technical accuracy and precedent are valid reasons to remove master/slave terminology from a codebase, they are of course not the only reason. Ahrens' own pull request describes this eloquently enough:

> *The horrible effects of human slavery continue to impact society. The casual use of the term "slave" in computer software is an unnecessary reference to a painful human experience.*

There should be nothing controversial about this, even if this were a drive-by pull request from a first-time contributor. Ahrens, of course, is anything but—he was one of the three founding Sun Microsystems ZFS developers beginning in 2001, and he remains a lead developer of the OpenZFS project today.

More importantly, it should be obvious that one person's impervious reaction to casual slavery-based analogies does not negate another person's experiences with slavery's historical

reality and its ongoing generational effects.

Ahrens' pull request has been reviewed by fellow lead developers Brian Behlendorf and Ryan Moeller and merged into the OpenZFS project repository.

https://arstechnica.com/?p=1683434

3M sues price-gougers who used Amazon to sell masks at 1,800% markup



Enlarge / The (replica) disembodied marble head of David probably didn't need a 3M mask, but he nonetheless looked fashionable sporting it in the window of a jewelry shop in

Switzerland in March 2020.

reader comments

91 with 59 posters participating, including story author

Share this story

3M—which manufactures N95 filtration masks that have been in high demand since the COVID-19 pandemic began—is suing merchants who used Amazon to sell 3M and counterfeit masks for more than 18 times their standard price.

A group of third-party merchants on Amazon "operated an illegal scheme to advertise and sell counterfeit, damaged, deficient, or otherwise altered respirators" to customers, 3M alleges in the complaint (PDF), filed in federal court in California.

3M has drastically increased its production of N95 respirator masks, the company says, but has kept its pricing between $0.63 and $3.40 per mask, depending on the model. The resellers in the suit, however, were allegedly selling a model that has a typical list price of $1.27 for for an average of $23.21 per mask, more than 18 times higher than 3M's price.

Amazon has already taken down the listings in question, 3M notes in the suit, but due to the way Amazon's third-party marketplace works, "banned" goods and sellers pop back up all the time. This case is likely to be no different, 3M claims, writing that the defendants have a history of launching "multiple front entities to perpetuate their unlawful activities" and adding that the defendants will probably keep doing it "until they are enjoined by this court."

3M seeks financial penalties against the resellers but says any monetary awards it receives "will be donated to charitable COVID-19 relief efforts."

The company has filed more than a dozen similar lawsuits in recent months, The Wall Street Journal notes. “The lawsuits are one tool in our tool kit to go after this kind of activity,” Kevin Rhodes, deputy general counsel for 3M, told the WSJ.

Price gouging for critical protective gear became rampant on US online platforms in February and March as the spread of the novel coronavirus caused a massive spike in demand. Suppliers couldn’t keep up, and so prices rose sharply for goods such as disposable gloves, masks, and hand sanitizer.

eBay outright banned listings for masks, hand sanitizers, and disinfectant wipes in early March amid rampant price-gouging and potential fraud. Amazon did not follow suit, instead turning to algorithmic detection and consumer complaints to remove problem listings.

More than 30 states’ attorneys general late in March asked online retailers, including Amazon, to take stronger, more proactive action against price-gouging merchants. “Rather than playing whack-a-mole to stop price gouging after it has already occurred,” the attorneys general wrote, “online retail platforms should prevent unconscionable price increases from occurring in the first place by creating and enforcing strong policies.”

https://arstechnica.com/?p=1682665

Researchers say online voting

tech used in 5 states is fatally flawed



Enlarge / Voting machines are shown at a polling location on June 9, 2020 in West Columbia, South Carolina.
Sean Rayford/Getty Images

reader comments

113 with 54 posters participating, including story author

Share this story

OmniBallot is election software that is used by dozens of jurisdictions in the United States. In addition to delivering ballots and helping voters mark them, it includes an option for online voting. At least three states—West Virginia, Delaware, and New Jersey—have used the technology or are planning to do so in an upcoming election. Four local jurisdictions in Oregon and Washington state use the online

voting feature as well. But new research from a pair of computer scientists, MIT's Michael Specter and the University of Michigan's Alex Halderman, finds that the software has inadequate security protections, creating a serious risk to election integrity.

Democracy Live, the company behind OmniBallot, defended its software in an email response to Ars Technica. "The report did not find any technical vulnerabilities in OmniBallot," wrote Democracy Live CEO Bryan Finney.

This is true in a sense—the researchers didn't find any major bugs in the OmniBallot code. But it also misses the point of their analysis. The security of software not only depends on the software itself but also on the security of the environment on which the system runs. For example, it's impossible to keep voting software secure if it runs on a computer infected with malware. And millions of PCs in the United States are infected with malware.

The issue has particular urgency right now because the ongoing COVID-19 pandemic is forcing election officials to make significant changes to election procedures. Right now, most jurisdictions using the OmniBallot software don't use its "electronic ballot delivery" feature. But enabling the feature would require little more than a configuration change. There's a risk that election officials, under pressure to make remote voting easier, will decide to enable the software's online voting feature for this November's general election.

How OmniBallot works

Experimenting with a live election system would be unethical and likely illegal. Instead, Specter and Halderman obtained a copy of the OmniBallot software, reverse-engineered it, and then created new server software that mimicked the behavior of the real server. This allowed them to experiment with the software without risking interference with a real election.

OmniBallot offers a number of different capabilities that state election officials have the option to offer to voters. The most basic is a blank ballot delivery feature that will provide a voter with a PDF ballot that can be printed out and mailed back to the polling place.

Jurisdictions can also offer a ballot-marking feature, which will mark a ballot on the voter's behalf before it's printed out. This can enable blind voters to fill out a ballot independently. It can also prevent overvotes (voting for two or more candidates) and warn voters about undervotes (failing to vote in a race).

But Specter and Halderman argue that this capability comes with some added risks. Malicious software could be programmed to switch votes some fraction of the time. Theoretically, voters are supposed to check that the votes are correct before mailing in their ballot, but research suggests voters are lax about doing so. One study by Halderman and others found that only 6.6 percent of voters in a realistic mock election reported a changed vote to election supervisors.

By default, the software generates the marked ballot PDF on an OmniBallot server, not on the user's own device. This creates an unnecessary risk to the privacy of the voter's ballot, Specter and Halderman argue, since it means that Democracy Live gets an unnecessary copy of the voter's votes.

Fortunately, Democracy Live also offers an option for client-side ballot marking. Andrew Appel, a computer scientist at Princeton, told Ars that this option was added at the insistence of California officials who objected to server-side ballot marking. When this option is chosen by election administrators, the ballot is marked on the user's own device, without sharing the data with Democracy Live's servers. The computer scientists recommend that all jurisdictions using OmniBallot's ballot marking feature switch to the client-side version of the software.

The problems with online voting

While there are some security concerns with ballot-marking software, the researchers say that these problems pale in comparison to security vulnerabilities of OmniBallot's "electronic ballot delivery" system.

The fundamental problem is that the complexity and opacity of online voting systems creates numerous opportunities for a hacker to tamper with a ballot during the submission process. Malware on the client device could modify the ballot before it's transmitted to Democracy Live's servers. OmniBallot is built on Amazon Web Services using JavaScript libraries delivered by Google and Cloudflare. So hackers or malicious insiders at any of these companies could potentially alter ballots if they had access to one of these companies' systems.

And the nature of online voting means there's no reliable way for a voter to verify that a ballot was transmitted correctly. Software engineers have developed theoretical designs for voting systems with end-to-end security. These systems use sophisticated cryptography to enable voters to cryptographically verify that their vote has been counted correctly. But Democracy Live doesn't do anything like that. In their paper, Specter and Halderman describe how an attacker could exploit the lack of end-to-end verification.

"The web app would show a ballot containing the selections the voter intended, but the ballot that got cast would have selections chosen by the attacker," they write. "The attack would execute on the client, with no unusual interactions with Democracy Live, so there would be no way for the company (or election officials) to discover it."

Auditing doesn't fix the problem

Democracy Live conducts post-election audits using Amazon's

AWS CloudTrail software to verify that no Democracy Live employees abused their access to company servers. These checks could detect some forms of election tampering, but Specter and Halderman point out that they are far from foolproof.

These methods wouldn't detect any attacks executed from the client side. If malware on a user's PC modified the user's ballot before sending it to Democracy Live's servers, that wouldn't show up in the CloudTrail logs. If someone with access to Google or Cloudflare servers delivered malicious JavaScript libraries to OmniBallot users, that wouldn't show up in AWS logs. Someone with administrative access to Amazon's servers might be able to modify Democracy Live's software in a way that wouldn't show up in the logs.

Of course, most of these attacks wouldn't be trivial to pull off. Google, Amazon, and Cloudflare are three of the most sophisticated software companies in the world and take elaborate precautions to defend their systems. The audit I linked to above is from an election for the King County Conservation District. It's farfetched that anyone would go to so much trouble to attack such a low-stakes election.

But sophisticated attacks would become far more plausible if the software were used to elect members of Congress and even the president. In that case, we can imagine foreign governments like Russia or China being willing to invest significant resources to compromise election results in a way that's difficult to detect. We don't know the full extent of these countries' offensive capabilities, of course. But it's reasonable to think that they'd be able to compromise OmniBallot's software in ways that wouldn't be revealed in a post-election audit.

To be fair to Democracy Live, the issues the researchers highlighted aren't unique to the OmniBallot software. Rather, there's an overwhelming consensus among computer security experts that Internet-based voting is a bad idea in general.

Halderman and Specter cite a 2018 report from the National Academies of Sciences, Engineering, and Medicine that found that “no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.”

https://arstechnica.com/?p=1682291

Ajit Pai caves to SpaceX but is still skeptical of Musk’s latency claims



Getty Images | Yuichiro Chino

reader comments

123 with 76 posters participating

Share this story

The Federal Communications Commission has reversed course on whether to let SpaceX and other satellite providers apply for rural-broadband funding as low-latency providers. But Chairman Ajit Pai said companies like SpaceX will have to prove they can offer low latencies, as the FCC does not plan to "fund untested technologies."

Pai's original proposal classified SpaceX and all other satellite operators as high-latency providers for purposes of the funding distribution, saying the companies haven't proven they can deliver latencies below the FCC standard of 100ms. Pai's plan to shut satellite companies out of the low-latency category would have put them at a disadvantage in a reverse auction that will distribute $16 billion from the Rural Digital Opportunity Fund (RDOF).

But SpaceX is launching low-Earth-orbit (LEO) satellites in altitudes ranging from 540km to 570km, a fraction of the 35,000km used with geostationary satellites, providing much lower latency than traditional satellite service. SpaceX told the FCC that its Starlink service will easily clear the 100ms cutoff, and FCC Commissioner Michael O'Rielly urged Pai to let LEO companies apply in the low-latency tier.

The FCC voted to approve the updated auction rules yesterday. The final order isn't public yet, but it's clear from statements by Pai and other commissioners that SpaceX and other LEO companies will be allowed to apply in the low-latency tier. The satellite companies won't gain automatic entry into the low-latency tier, but they will be given a chance to prove that they can deliver latencies below 100ms.

"I am grateful to the chairman for agreeing to expand

eligibility for the low-latency performance tier and change language that was prejudicial to certain providers," O'Rielly said at yesterday's FCC meeting. "While a technology-neutral policy across the board may have been more effective in promoting innovation and maximizing the value of ratepayer investments, I recognize that a balancing act was necessary to reach the current disposition."

Pai: FCC will apply "very close scrutiny"

Pai said that he agreed to the change "at the request of one of my fellow commissioners." The final rules "don't entirely close the door on low-Earth orbit satellite providers bidding in the low-latency tier," Pai continued. "However, it is also important to keep in mind the following point: The purpose of the Rural Digital Opportunity Fund is to ensure that Americans have access to broadband, no matter where they live. It is not a technology incubator to fund untested technologies. And we will not allow taxpayer funding to be wasted. A new technology may sound good in theory and look great on paper. But this multi-billion-dollar broadband program will require 't's to be crossed—not fingers. So any such application will be given very close scrutiny."

When contacted by Ars today, Pai's office confirmed that "the commission modified the draft to permit LEO service providers to apply to bid in the low-latency tier instead of limiting them to the high-latency tier, and staff will be closely reviewing all applications to ensure they can meet the FCC's performance requirements for service providers."

SpaceX is aiming to provide service later this year, and CEO Elon Musk has said the company is aiming for latency below 20ms.

Commissioner Geoffrey Starks supported the low-latency change

in his statement:

> *I appreciate Commissioner O'Rielly's work in revising this Public Notice to eliminate the categorical bar on low-Earth orbit satellite systems bidding in the low-latency tier, especially now that we have evidence in the record that those systems can meet the 100-millisecond latency standard. At the same time, I see no need for the Public Notice's predictive judgments about the merits of short-form applications from low-Earth orbit satellite operators. As I have stated previously, next-generation satellite broadband holds tremendous technological promise for addressing the digital divide and is led by strong American companies with a lengthy record of success. Commission staff should evaluate those applications on their own merits.*

Pai and O'Rielly are Republicans, while Starks is part of the FCC's Democratic minority.

SpaceX excluded from gigabit tier

The $16 billion in phone and broadband subsidies will be distributed in a reverse auction scheduled to begin on October 29. ISPs can seek funding in census blocks where no provider offers home-Internet speeds of at least 25Mbps downstream and 3Mbps upstream. The $16 billion will be distributed over 10 years, so ISPs that get funded will collect a total of about $1.6 billion a year and face requirements to deploy broadband service to a certain number of homes and businesses.

Pai's auction rules also shut SpaceX and other satellite operators out of applying for funding in the gigabit tier. SpaceX could still apply for funding in the 100Mbps-and-below categories, but the auction will prioritize applications in the gigabit category. SpaceX has said in the past that it would offer gigabit speeds, but the company seems to have only objected to the latency restriction.

The commissioners' statements did not mention any change to the policy excluding all satellite providers from the gigabit tier. The gigabit tier requires 1Gbps download speeds and 500Mbps upload speeds, which in practice may restrict the category primarily to fiber-to-the-home providers or cable companies that adopt full-duplex DOCSIS technology.

Pai said the FCC is allowing fixed-wireless and DSL providers to apply in the gigabit tier but said that "commission staff will conduct a careful, case-by-case review of applications to ensure that bidders will be able to meet required performance obligations." There's apparently still no allowance for LEO-satellite providers to bid in the gigabit tier.

Technology neutrality

O'Rielly said he wanted the FCC to let all types of providers apply for all speed tiers, with the requirement that they demonstrate their ability to deliver those speeds:

> *One of the key principles that I have sought to advance, in both the auction context and elsewhere, is the concept of technology neutrality… in the auction context, it involves crafting rules that offer a fair shot to innovators across all sectors and don't unduly tilt the playing field toward particular providers. Therefore, I would have preferred an auction design without up-front technology restrictions; all interested providers should have the opportunity to demonstrate whether they can meet our speed and latency benchmarks at the short-form application stage. After all, the whole point of the auction is to support the deployment of broadband services that wouldn't otherwise exist in the absence of subsidies.*

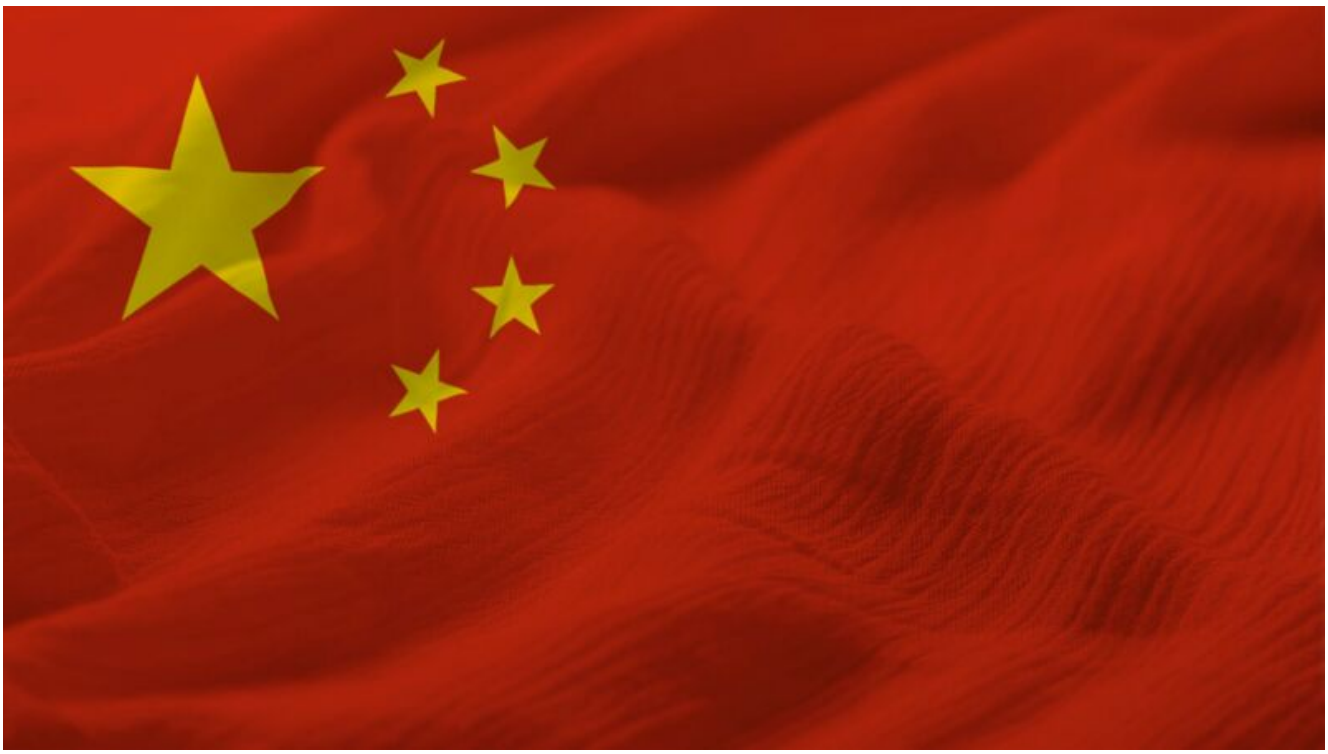
Before Pai changed his mind, the draft plan said, "In the absence of a real world example of a non-geostationary orbit satellite network offering mass market fixed service to

residential consumers that is able to meet our 100ms round trip latency requirements, Commission staff could not conclude that such an applicant is reasonably capable of meeting the Commission’s low latency requirements, and so we foreclose such applications.”

SpaceX met with commission staff over the last few days of May, telling them that its broadband system “easily clears the commission’s 100ms threshold for low-latency services, even including its ‘processing time’ during unrealistic worst-case scenarios.” We contacted SpaceX today about the low-latency change and will update this story if we get a response.

https://arstechnica.com/?p=1682670

FCC failed to monitor Chinese telecoms for almost 20 years: Senate report



Enlarge / The flag of China.

reader comments

29 with 28 posters participating

Share this story

The Federal Communications Commission and other US agencies have failed to properly oversee Chinese telecom companies that operate in the United States, according to a bipartisan Senate report released today.

After a year-long investigation, the staff report by the US Senate's Permanent Subcommittee on Investigations "found that the FCC and 'Team Telecom'—an informal group comprised of officials from the Departments of Justice, Homeland Security, and Defense—have failed to monitor these three Chinese government-owned carriers," a joint announcement by the subcommittee's Republican and Democratic leaders said. The three carriers the subcommittee referred to are China Telecom Americas (CTA), China Unicom Americas (CUA), and ComNet USA. The companies "operated in the US for nearly 20 Years with little to no oversight from the federal government," the

senators' announcement said.

"The Chinese government engages in cyber and economic espionage efforts against the United States and may use telecommunications carriers operating in the United States to further these efforts," the report said.

The report comes two months after the FCC stepped up its scrutiny of telecom companies controlled by the Chinese government. The FCC issued orders to China Telecom, China Unicom, ComNet, and ComNet owner Pacific Networks, directing them "to explain why the Commission should not start the process of revoking their domestic and international section authorizations enabling them to operate in the United States." But the FCC and other agencies had previously failed to exercise proper oversight of these companies, the Senate report said.

The lack of oversight described in the report occurred during both Republican and Democratic administrations. "An FCC spokesman said the commission looks forward to reviewing the Senate report," according to a Reuters article today.

China Telecom faced little US review

Team Telecom—the informal grouping of the Department of Justice, Department of Homeland Security, and Department of Defense—evaluates national security and law enforcement concerns about telecom carriers and makes recommendations to the FCC.

A section of the report on China Telecom says the company "is ultimately owned by the Chinese government" and has operated in the US for nearly 20 years. The company's "US operations provide opportunities for China to engage in economic espionage against the United States," the report said.

When China Telecom applied for authorization to operate in the US in 2001, Team Telecom did not object, and the FCC thus "streamlined the application and approved it two weeks after accepting it for filing." The original authorization "limited CTA to providing international services between the United States and international points, other than China," but the FCC shortly thereafter approved another "authorization to serve as a facilities-based carrier between the United States and China."

After those two authorizations, "Team Telecom did not interact with CTA between 2002 and 2007" and "documents suggest that Team Telecom may not have understood that, prior to 2007, CTA was providing services between the United States and China," the Senate report said.

CTA notified the FCC of a change in ownership in July 2007, though this "change had no impact on CTA's ultimate ownership" by the Chinese government, the report said. The restructuring triggered a new FCC review, in which CTA told the agency that "its customers were split among enterprise customers and other telecommunications carriers throughout the United States." CTA also "provided Team Telecom with a list of its top three executives—all of whom were Chinese nationals."

"Team Telecom determined that security measures were warranted," and "the parties negotiated a three-page security agreement" that among other things was intended "to prevent unauthorized access to, or disclosure of the content of, communications or US records."

But the US government barely followed up with CTA after that agreement. "Team Telecom's oversight of CTA since 2007 has consisted of two site visits and intermittent email communication," the Senate report said.

"When asked to explain the lack of oversight during this period, despite the security agreement being in effect, Team

Telecom officials pointed to the security agreement, noting that because it was broadly written, demonstrating compliance was straightforward," the report said.

Hands-off approach ends

Team Telecom finally began "substantive oversight of CTA" in 2017, in part with a site visit that "identified concerns related to CTA's storage of US customer data." The report also said there have been "allegations of China Telecom hijacking communications data dat[ing] back to 2010," but "Team Telecom did not question CTA about these reports until January 2019."

CTA denied the allegations, and "Team Telecom appears to have relied on CTA's written representations regarding the alleged incidents. Team Telecom provided no records or explanation of it conducting further interviews, requesting or reviewing additional documentation, or otherwise questioning CTA's assertions," the Senate report said.

The hands-off approach changed by April 2020, when Team Telecom "recommended the FCC revoke and terminate CTA's Section 214 authorizations because of 'substantial and unacceptable' national security risks." Team Telecom "warned that CTA's facilities-based authorizations allow it to request interconnections with US carriers" and that CTA had "already established relationships with major US carriers, including Verizon, CenturyLink, and AT&T."

"Neither Verizon, AT&T, nor CenturyLink maintains any mitigation or other agreement focused on network security with CTA or its parent company," though these US carriers "maintain company-wide cybersecurity defenses that apply to all external traffic," the Senate report said.

The report says that "CTA is untrustworthy," arguing that the company's "delayed response" to document and information requests in April 2018 "called into question CTA's willingness

to comply with the security agreement." Team Telecom also found that "CTA had breached the security agreement by failing to implement a formal written information security policy prior to December 1, 2018."

China Telecom denies "purely hypothetical risks"

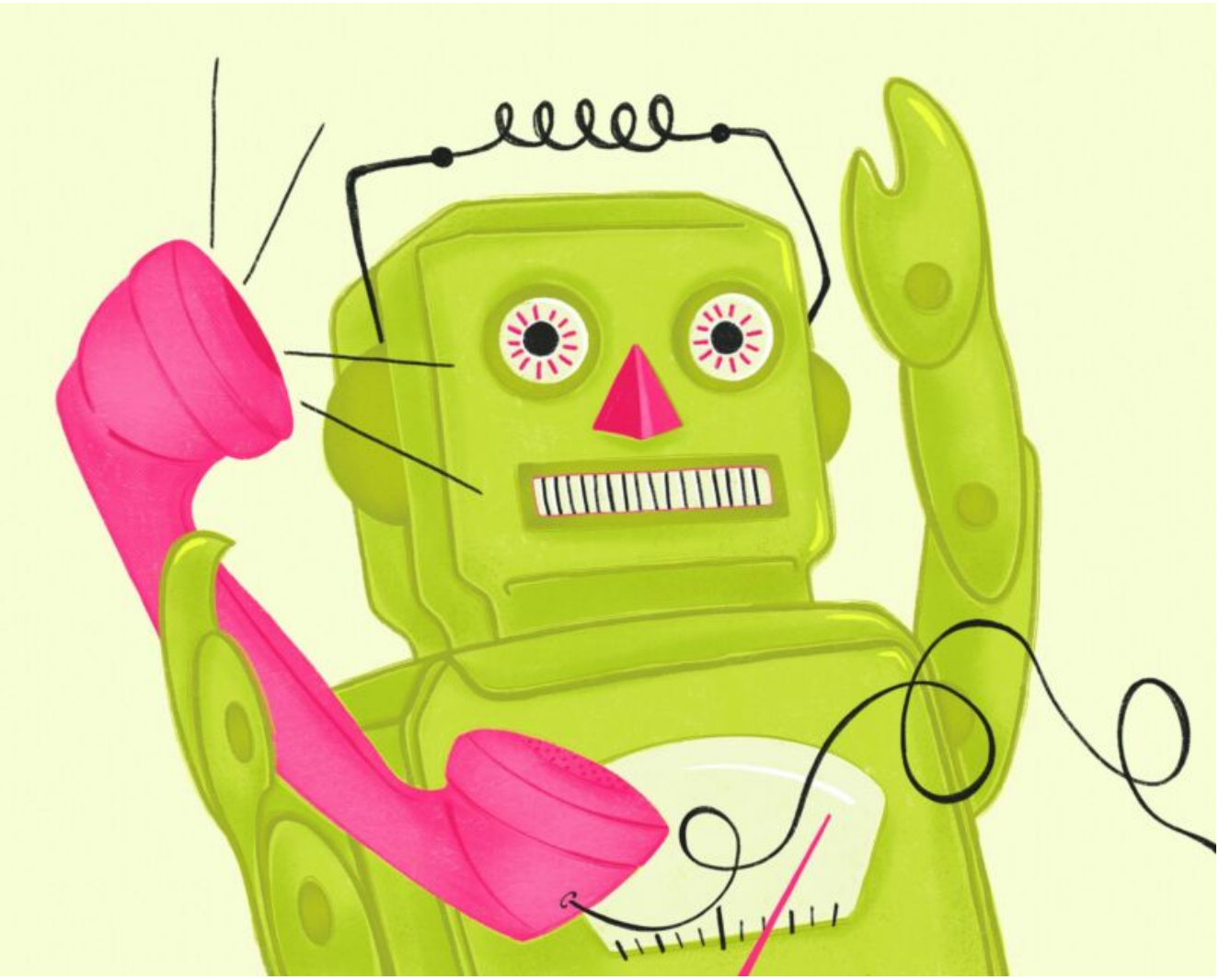
The FCC is still considering the Team Telecom recommendation to revoke CTA's authorizations. CTA disputed the allegations in an FCC filing yesterday, saying that the FCC "inquiry unfairly and improperly places the burden on CTA to prove a negative regarding unspecified national security concerns about 'exploitation' and 'influence' of the Chinese government. These vague terms are left undefined in the Order or, to CTA's knowledge, anywhere in the FCC's rules or decisions." CTA's redacted filing says the company "serv[es] many US customers" and employs "many US citizens and permanent residents."

"[E]ven if the commission were to credit the purely hypothetical risks suggested by the [Team Telecom] recommendation, none of which have actually occurred, the commission would have to consider whether there is a remedy short of revocation that would foreclose these risks while preserving the services used by thousands of CTA customers. Team Telecom's summary refusal even to consider potential mitigation measures is not justified," China Telecom wrote.

CTA also wrote that "the Communications Act and Commission precedent permit revocation of CTA's authorizations only if there is clear and convincing evidence of egregious misconduct by CTA."

https://arstechnica.com/?p=1682529

1 billion robocalls net $225M FCC fine that will likely never be collected



Getty Images | Juj Winn

reader comments

69 with 38 posters participating

Share this story

The Federal Communications Commission today proposed a $225 million fine for health-insurance telemarketers who "made approximately 1 billion spoofed robocalls across the country during the first four and a half months of 2019." But the FCC's track record in collecting on proposed fines is so poor that the fine is unlikely to ever be collected at anywhere close to the proposed amount.

Rising Eagle, a Texas-based health insurance telemarketer, made 1 billion calls "on behalf of clients that sell short-term, limited-duration health insurance plans," the FCC said. Here's how the FCC described the robocalls:

> *The robocalls falsely claimed to offer health insurance plans from well-known health insurance companies such as Aetna, Blue Cross Blue Shield, Cigna, and UnitedHealth Group. For example, one call stated: "Are you looking for affordable health insurance with benefits from a company you know? Policies have all been reduced nationwide such as Cigna, Blue Cross, Aetna, and United just a quick phone call away. Press 3 to get connected to a licensed agent or press 7 to be added to the Do Not Call list." If they did press 3, consumers were transferred to a call center with no affiliation to the named companies, where call center representatives then would attempt to convince the consumer to purchase an insurance product sold by one of Rising Eagle's clients. Rising Eagle's largest client, Health Advisors of America, was sued by the Missouri Attorney General for telemarketing violations in February 2019.*

The proposed $225 million fine is for "apparent violations by John C. Spiller and Jakob A. Mears, who used business names including Rising Eagle and JSquared Telecom," the FCC said. It's a proposed fine because that's how the FCC process works: the commission issues a Notice of Apparent Liability for

Forfeiture containing allegations, and the alleged robocaller is given an opportunity to respond and provide evidence. The process can end in a settlement or a fine that cannot exceed the proposed amount of $225 million. The amount of $225 million would be the largest-ever FCC fine, but the commission has a disappointing track record in collecting on these proposed penalties.

“Over the last several years the FCC has levied hundreds of millions in fines against robocallers just like the folks we have here today. But so far collections on these eye-popping fines have netted next to nothing,” FCC Commissioner Jessica Rosenworcel, one of two Democrats on the Republican-majority commission, said in a statement sent to reporters today. “In fact, it was last year that The Wall Street Journal did the math and found that we had collected no more than $6,790 on hundreds of millions in fines. Why? Well, one reason is that the FCC looks to the Department of Justice to collect on the agency’s fines against robocallers. We need them to help. So when they don’t get involved—as here—that’s not a good sign.”

According to the FCC press release, “Spiller admitted to the USTelecom Industry Traceback Group that he knowingly called consumers on the Do Not Call list as he believed that it was more profitable to target these consumers. He also admitted that he made millions of calls per day, and that he was using spoofed numbers.”

The FCC investigation into Rising Eagle found that its calls “were spoofed in order to deceive consumers, targeted millions of Do Not Call list participants, and were received on many wireless phones without prior consumer consent.” The Rising Eagle “scam also caused the companies whose caller IDs were spoofed to become overwhelmed with angry call-backs from aggrieved consumers. At least one company was hit with several lawsuits because its number was spoofed, and another was so overwhelmed with calls that its telephone network became unusable.”

Spoofing of Caller ID lets callers hide their identities by making phone calls appear to come from other numbers. The FCC, following instructions from Congress, is mandating that carriers deploy the STIR/SHAKEN framework that uses digital certificates to verify the accuracy of Caller ID. The FCC has also been pressuring US-based carriers to stop accepting suspicious foreign call traffic, but the robocall problem is so big that it may never be fully solved.

Update at 3:30pm ET: After this story published, FCC Chairman Ajit Pai announced that seven state attorneys general today sued Rising Eagle and the other robocallers in the case in US District Court for the Southern District of Texas. The court complaint seeks a permanent injunction and damages of up to $3,000 for each violation.

https://arstechnica.com/?p=1682403