Amazon: Trump used “improper pressure” to block AWS from DOD cloud contract



Enlarge / The JEDI contract is central to DOD’s efforts to rapidly adopt cloud technology. But the winner-take-all contract offer has been controversial from the start—and now Amazon claims President Trump put a whole lot more than a finger on the scales to ensure AWS lost.
Department of Defense

reader comments

143 with 90 posters participating

Share this story

In a redacted filing released today by the US Federal Court of Claims, attorneys for Amazon asserted that Amazon Web Service’s loss of the Department of Defense Joint Enterprise Defense Infrastructure (JEDI) cloud computing contract to Microsoft’s Azure was the result of “improper pressure from President Donald J. Trump, who launched repeated public and

behind-the-scenes attacks to steer the JEDI Contract away from AWS to harm his perceived political enemy—Jeffrey P. Bezos, founder and CEO of AWS' parent company, Amazon.com, Inc. ("Amazon"), and owner of the Washington Post."

The suit cites Trump's instructions to former Secretary of Defense James Mattis to "screw Amazon" out of the contract, as recounted by Mattis' former chief speechwriter, and numerous other incidents of direct interference by Trump in the contract competition, including ordering an "independent" review of the contract by Defense Secretary Mark Esper in August of 2019.

JEDI was awarded to Microsoft in October. The $10 billion contract is for a DOD-wide enterprise Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service(PaaS) program providing compute and storage services—including delivering them to the "tactical edge," giving troops in the field access to critical data. The initial expenditure, scheduled for the first year of the contract, would be just $1 million—but it would be followed by a base two-year ordering period and up to eight years of optional extensions out to 2029, with a capped value of $10 billion.

- The before (left) and (hopefully) after (right) architecture designs of DOD cloud.
- All sorts of services are supposed to be part of JEDI, at classifications up to Top Secret.
- Only $1 million is guaranteed—so that $10 billion could be a pipe dream if the winner can't deliver.

Because of the scale of the contract, AWS was long assumed to be the front-runner—AWS already provides the DOD with cloud services and other government agencies that meet most of the security requirements set out by the JEDI contract. But Microsoft's Azure was also a strong contender, and the DOD's internal cloud capabilities (provided by the Defense

Information Systems Agency) have relied heavily on Microsoft technology. And Amazon's attorneys claim that after Trump injected himself into the procurement discussion, the DOD "took numerous actions to systematically remove the advantages of AWS' technological and experiential superiority and artificially level the playing field between AWS and its competitors, including Microsoft."

The filing cites as an example the DOD's decision in mid-2018 to not evaluate past performance as part of the competition in violation of Federal Acquisition Regulation (FAR) requirements—when "only AWS possessed [past performance] with regard to a contract remotely comparable to the size and complexity of JEDI."

"These errors, however, were not merely the result of arbitrary and capricious decision making," the filing states. "DoD's substantial and pervasive errors are hard to understand and impossible to assess separate and apart from the President's repeatedly expressed determination to, in the words of the President himself, 'screw Amazon.'" As a result, Amazon's attorneys asserted, "Basic justice requires reevaluation of proposals and a new award decision," and the court should decide "whether the President of the United States should be allowed to use the budget of DoD to pursue his own personal and political ends."

https://arstechnica.com/?p=1630099

Bernie Sanders vows to break

up huge ISPs and regulate broadband prices



Enlarge / Bernie Sanders speaks to the Organic Farmers Association on December 05, 2019 in Story City, Iowa.
Getty Images | Win McNamee

reader comments

129 with 82 posters participating

Share this story

Presidential candidate and Vermont Senator Bernie Sanders yesterday released a plan to overhaul the US broadband market by breaking up giant providers, outlawing data caps, regulating broadband prices, and providing $150 billion to build publicly owned networks.

“The Internet as we know it was developed by taxpayer-funded

research, using taxpayer-funded grants in taxpayer-funded labs," the Sanders plan said. "Our tax dollars built the Internet, and access to it should be a public good for all, not another price-gouging profit machine for Comcast, AT&T, and Verizon."

If enacted, Sanders' "High-Speed Internet for All" plan would be the polar opposite of the Trump administration's treatment of broadband companies and far more aggressive than the regulatory approach of the Obama administration. Sanders pledged to "use existing antitrust authority to break up Internet service provider and cable monopolies," specifically by "bar[ring] service providers from also providing content and unwind anticompetitive vertical conglomerates."

Perhaps most notably, this could force Comcast to divest NBCUniversal and force AT&T to divest Time Warner. Of course, a US president can't simply issue an order to break up these companies. But if Sanders is elected, he could nominate Department of Justice officials who are likely to file antitrust lawsuits against the companies that dominate the broadband industry.

Bring back Title II regulation

Sanders also pledged to regulate broadband providers as common carriers under Title II of the Communications Act, reinstate net neutrality rules, and impose other pro-consumer rules. This could be achieved via legislation, appointments of aggressive regulators to the Federal Communications Commission, or a combination of both.

Sanders said he would "eliminate data caps and ban throttling" and "instruct the FCC to regulate broadband Internet rates so households and small businesses are connected affordably." This would include a requirement "that all Internet service providers offer a Basic Internet Plan that provides quality broadband speeds at an affordable price."

The FCC is an independent agency, so it wouldn't have to do what Sanders says. But if Sanders was president, he could nominate commissioners and appoint a chairperson who is likely to carry out his wishes.

$150 billion

Sanders also proposed investing heavily in infrastructure, particularly in government-run networks. He pledged to "provide $150 billion through the Green New Deal in infrastructure grants and technical assistance for municipalities and/or states to build publicly owned and democratically controlled, co-operative, or open-access broadband networks."

Sanders vowed to preempt 19 state laws that limit the spread of municipal broadband. That could require help from Congress, as the Obama-era FCC's attempt to preempt such laws was overturned in court.

Presidential candidate Elizabeth Warren has proposed an $85 billion broadband plan, while candidate Joe Biden has proposed $20 billion for rural broadband.

Many US residents lack fast Internet service today because broadband monopolies "don't provide service to anyone who can't afford it, or install it in areas where it won't make them as much money as their shareholders demand," the Sanders plan said. Meanwhile, broadband monopolies "exploit their dominant market power to gouge consumers and lobby government at all levels to keep out competition."

Sanders compared his plan to President Franklin D. Roosevelt's "promise to deliver electricity to every home in America in 1935, a time when 90 percent of rural households lacked it."

Sanders' $150 billion proposal includes a Department of Agriculture Rural Utility Service program "to provide capital

funding to connect all remote rural households and businesses and upgrade outdated technology and infrastructure, prioritizing funding for existing co-ops and small rural utilities." Sanders said that $7.5 billion should be set aside for tribal areas and that all public housing should provide free broadband to residents.

Sanders said the $150 billion investment will "ensure that communities stay connected during natural disasters." Sanders also proposed a full review of broadband networks to make sure they are "resilient to the effects of climate change."

Sanders aims to lower prices

US government plans for broadband often focus on network access without talking much about lowering prices. Sanders wants to do both. His plan said:

> *Large Internet service providers have enjoyed government funding, protection from competition, and light regulation while gouging customers with some of the highest prices for service in the world. Bernie will regulate these providers like a utility. The FCC will review prices and regulate rates where necessary, ensuring areas without competition aren't able to run up prices.*

Moreover, Sanders proposed eliminating the hidden fees broadband providers use to make the actual cost higher than their advertised rates. ISPs would have to "clearly state the cost of service" and not impose "unexpected rate increases" or "service termination fees."

Sanders also wants the FCC to define broadband as a minimum of 100Mbps download speeds and 10Mbps uploads, instead of the current 25Mbps down and 3Mbps up. Sanders would also "reinstate and expand privacy protection rules," reversing the Trump-era decision to eliminate broadband-privacy rules.

https://arstechnica.com/?p=1629483

Jury sides with Elon Musk in “pedo guy” defamation case



Enlarge / Elon Musk leaves a Los Angeles federal court on Tuesday December 3, 2019.
Apu Gomes/Getty Images

reader comments

267 with 139 posters participating

Share this story

A Los Angeles federal jury has found Elon Musk not liable for

defamation in a lawsuit brought by British caver Vernon Unsworth. Musk dubbed Unsworth a “pedo guy” in a tweet last year, but argued in court that he meant this as a generic insult—not as an accusation that Unsworth was a pedophile.

“My faith in humanity is restored,” Musk reportedly said on his way out of court.

Musk and Unsworth have been trading insults since last July, when Unsworth mocked a miniature submarine SpaceX engineers created to help rescue a dozen boys trapped in a cave in Thailand (it didn’t arrive in time to be useful). In an interview with CNN, Unsworth said that Musk should “stick his submarine where it hurts.”

Musk responded with a tweet labeling Unsworth a “pedo guy” and vowing to prove that the submarine would have been able to squeeze through the narrowest passages in the cave.

A month later, Musk continued to needle Unsworth. “You don’t think it’s strange he hasn’t sued me?” he tweeted in August 2018.

Then Unsworth did sue him. The trial started on Tuesday with testimony from Musk.

Unsworth’s comments were “an unprovoked attack on what was a good-natured attempt to help the kids,” Musk told the court. “It was wrong and insulting, and so I insulted him back.”

“I knew he didn’t literally mean to sodomize me with a submarine, just as I didn’t literally mean he was a pedophile,” Musk said.

Unsworth’s lawyers argued that many people took Musk’s words literally, causing Unsworth “shame, mortification, worry, and distress.”

But the jury found Musk’s arguments more convincing. Or perhaps they simply didn’t view the feud as serious enough to

warrant cash damages.

“It was very clear,” one juror said, according to Buzzfeed reporter Ryan Mac. “I don’t want to have anything to do with this,” another added.

https://arstechnica.com/?p=1629307

Social media platforms leave 95% of reported fake accounts up, study finds



Enlarge / One hundred cardboard cutouts of Facebook founder and CEO Mark Zuckerberg stand outside the US Capitol in Washington, DC, April 10, 2018.

reader comments

54 with 44 posters participating

Share this story

It’s no secret that every major social media platform is chock-full of bad actors, fake accounts, and bots. The big companies continually pledge to do a better job weeding out organized networks of fake accounts, but a new report confirms what many of us have long suspected: they’re pretty terrible at doing so.

The report comes this week from researchers with the NATO Strategic Communication Centre of Excellence (StratCom). Through the four-month period between May and August of this year, the research team conducted an experiment to see just how easy it is to buy your way into a network of fake accounts and how hard it is to get social media platforms to do anything about it.

The research team spent €300 (about $332) to purchase engagement on Facebook, Instagram, Twitter, and YouTube, the report (PDF) explains. That sum bought 3,520 comments, 25,750 likes, 20,000 views, and 5,100 followers. They then used those interactions to work backward to about 19,000 inauthentic accounts that were used for social media manipulation purposes.

About a month after buying all that engagement, the research team looked at the status of all those fake accounts and found that about 80 percent were still active. So they reported a sample selection of those accounts to the platforms as fraudulent. Then came the most damning statistic: three weeks after being reported as fake, *95 percent* of the fake accounts were still active.

“Based on this experiment and several other studies we have conducted over the last two years, we assess that Facebook,

Instagram, Twitter, and YouTube are still failing to adequately counter inauthentic behavior on their platforms," the researchers concluded. "Self-regulation is not working."

Too big to govern

The social media platforms are fighting a distinctly uphill battle. The scale of Facebook's challenge, in particular, is enormous. The company boasts 2.2 billion *daily* users of its combined platforms. Broken down by platform, the original big blue Facebook app has about 2.45 billion monthly active users, and Instagram has more than one billion.

Facebook frequently posts status updates about "removing coordinated inauthentic behavior" from its services. Each of those updates, however, tends to snag between a few dozen and a few hundred accounts, pages, and groups, usually sponsored by foreign actors. That's barely a drop in the bucket just compared to the 19,000 fake accounts that one research study uncovered from one $300 outlay, let alone the vast ocean of other fake accounts out there in the world.

The issue, however, is both serious and pressing. A majority of the accounts found in this study were engaged in commercial behavior rather than political troublemaking. But attempted foreign interference in both a crucial national election on the horizon in the UK this month and the high-stakes US federal election next year is all but guaranteed.

The Senate Intelligence Committee's report (PDF) on social media interference in the 2016 US election is expansive and thorough. The committee determined Russia's Internet Research Agency (IRA) used social media to "conduct an information warfare campaign designed to spread disinformation and societal division in the United States," including targeted ads, fake news articles, and other tactics. The IRA used and uses several different platforms, the committee found, but its primary vectors are Facebook and Instagram.

Facebook has promised to crack down hard on coordinated inauthentic behavior heading into the 2020 US election, but its challenges with content moderation are by now legendary. Working conditions for the company's legions of contract content moderators are terrible, as repeatedly reported—and it's hard to imagine the number of humans you'd need to review literally trillions of pieces of content posted every day. Using software tools to recognize and block inauthentic actors is obviously the only way to capture it at any meaningful scale, but the development of those tools is clearly also still a work in progress.

https://arstechnica.com/?p=1628893

Kingpin of Evil Corp lived large. Now there's a $5 million bounty on his head



Enlarge / Screenshot of Justice Department website shows four pictures of same alleged criminal.

reader comments

39 with 29 posters participating

Share this story

Federal prosecutors have indicted the kingpin of Evil Corp, the name used by a cybercrime gang that used the notorious Dridex malware to drain more than $70 million from bank accounts in the US, UK, and other countries.

Maksim V. Yakubets, a 32-year-old Russian national who used the handle "Aqua," led one of the world's most advanced transnational cybercrime syndicates in the world, prosecutors said on Thursday. The crime group's alleged deployment of Dridex was one of the most widespread malware campaigns ever. The UK's National Crime Agency said the syndicate used the name Evil Corp.

Dridex was configured to target the customers of almost 300 different organizations in more than 40 countries by automating the theft of online banking credentials and other confidential information from infected computers. Over time, Dridex creators updated the malware to install ransomware. Previously known as Bugat and Cridex, Dridex used zeroday exploits and malicious attachments in emails to infect targets. The malware was designed to bypass antivirus and other security defenses.

Yakubets and another alleged Dridex operator, 38-year-old Igor Turashev, also from Russia, allegedly used the captured banking credentials to order electronic money transfers from compromised accounts. Prosecutors said the men funneled the stolen funds into the accounts of money mules who would move the funds into other accounts or convert them to cash and smuggle it overseas. Yubets was the leader of the crime group, prosecutors said. Turashev allegedly handled a host of roles, including system administration, management of an internal control panel, and oversight of a botnet that controlled infected computers.

Confiscated images and videos released by UK authorities show alleged members of Evil Corp living large. One photo shows Yakubets and his bride celebrating their 2017 wedding with a lavish chandelier above them. Other images and videos show off expensive sports cars.

- A photo from Yakubets' wedding in Moscow.
- A Lamborghini belonging to Maksim Yakubets parked outside Chianti Café.
- Evil Corp member Andrey Plotnitskiy with cash.
- A Lamborghini Huracan and an Audi R8 used by Evil Corp members outside Moscow State University.
- Nissan GTR used by Evil Corp member Dmitriy Smirnov with a Philipp Plein wrap.
- An Audi R8 belonging to an Evil Corp member. It's parked

outside Chianti Café, a location used by the group.

- Evil Corp member cars: Lamborghini Huracan belonging to Maksim Yakubets.
- Evil Corp group member Andrey Plotnitskiy standing in front of a Porsche.
- An Evil Corp member giving the finger to police.
- Evil Corp member Dmitriy Smirnov standing on his Nissan GTR and a Chevrolet Camaro.
- Another Evil Corp member.
- Evil Corp group members (left to right) Kirill Slovoddkoy, Dmitry Smirnov, and Denis Gusev on holiday in Dubai in 2013.

Yakubets also stands accused of providing "direct assistance" to the Federal Security Service of the Russian Federation, the KGB successor that's better known as the FSB.

"In addition to his leadership role within Evil Corp, Yakubets has also provided direct assistance to the Russian government," officials with the US Treasury Department said. "As of 2017, Yakubets was working for the Russian FSB, one of Russia's leading intelligence organizations that was previously sanctioned pursuant to E.O. 13694, as amended, on December 28, 2016."

https://arstechnica.com/?p=1628605

DOL's $400M pay-discrimination suit is

unconstitutional, Oracle argues



Enlarge / Regional headquarters of software company Oracle in San Jose, California, April 13, 2019.

reader comments

72 with 40 posters participating

Share this story

As a long-running Department of Labor suit against Oracle heads in front of a judge this week, Oracle is fighting back by arguing that the DOL's suit, alleging violation of labor laws, is unconstitutional.

The DOL filed suit against Oracle in 2017, alleging that the company had a broad, systemic pay discrepancy that underpaid women and people of color employed by the firm by a total $401

million in a four-year period. Analyses conducted by the department, as well as by independent third parties, found women were being paid between $13,000 and $20,000 less per year, on average, than their male peers.

The hearings in the case began today. The DOL is expected to call more than 20 current and former employees as witnesses in the case over the next week or two of proceedings.

This kind of complaint, however, does not go into the regular federal court system. Instead, it goes before an administrative law judge—a different office within the Department of Labor. More than 30 different federal agencies use this model, including the Federal Trade Commission, the Federal Communications Commission, and the Food and Drug Administration.

Just before Thanksgiving, Oracle, in its own words, filed a suit "challenging the legality of the system" of administrative law judges. That system, Oracle claims, violates both the US Constitution as well as several federal laws.

"The government's case rests on false allegations, cherry-picked statistics, and erroneous and radical theories of the law," Oracle said about the suit. "The Labor Department's nonsensical claims underscore the need for the federal courts to declare the Department of Labor's current enforcement system unconstitutional."

The backstory

The 2017 DOL complaint (PDF) alleged that white men employed by Oracle received significantly more pay than women, black, or Asian employees of the firm, even when controlling for "job title, full-time status, exempt status, global career level, job specialty, estimated prior work experience, and company tenure."

Between 2013 and the time the suit was filed in 2017, the DOL found, the salaries women received as compared to their male peers were between 2.71 and 8.41 standard deviations lower, depending on job category. The salary paid to black employees, adjusted for the same variables, had a standard deviation 2.10 lower than the compensation for white men, and for Asian employees the difference was -6.55. Oracle also showed hiring bias in certain roles, disproportionately staffing them with those (lower-paid) Asian employees, the DOL said, particularly individuals of Indian descent. In one six-month time span in 2013, 82 percent of hires in one job group were identified as Asian.

Three women who had by that point left their jobs with Oracle also filed a separate suit in 2017, alleging a pattern of gendered discrimination in pay and other unfair practices in violation of California labor law. The plaintiffs in that suit are seeking class-action status to represent a group of about 4,200 employees.

Oracle bites back

The DOL complaint not only seeks financial restitution for all the affected employees but also to make Oracle cancel its general contracts while being barred from taking on new ones. That would be an enormous blow for Oracle, which still relies on federal money despite recently missing out on a $10 billion contract with the Department of Defense. (Oracle is suing the DOD over the contract, which ultimately went to Microsoft.)

Against that backdrop, it is perhaps unsurprising that Oracle sued back. In its complaint, (PDF), Oracle called the DOL action “unprecedented overreach” and argued that the system is “coercive” and self-serving.

“Without authority from any Act of Congress—indeed, in contravention of congressional legislation—a group of unelected, unaccountable, and unconfirmed administrative

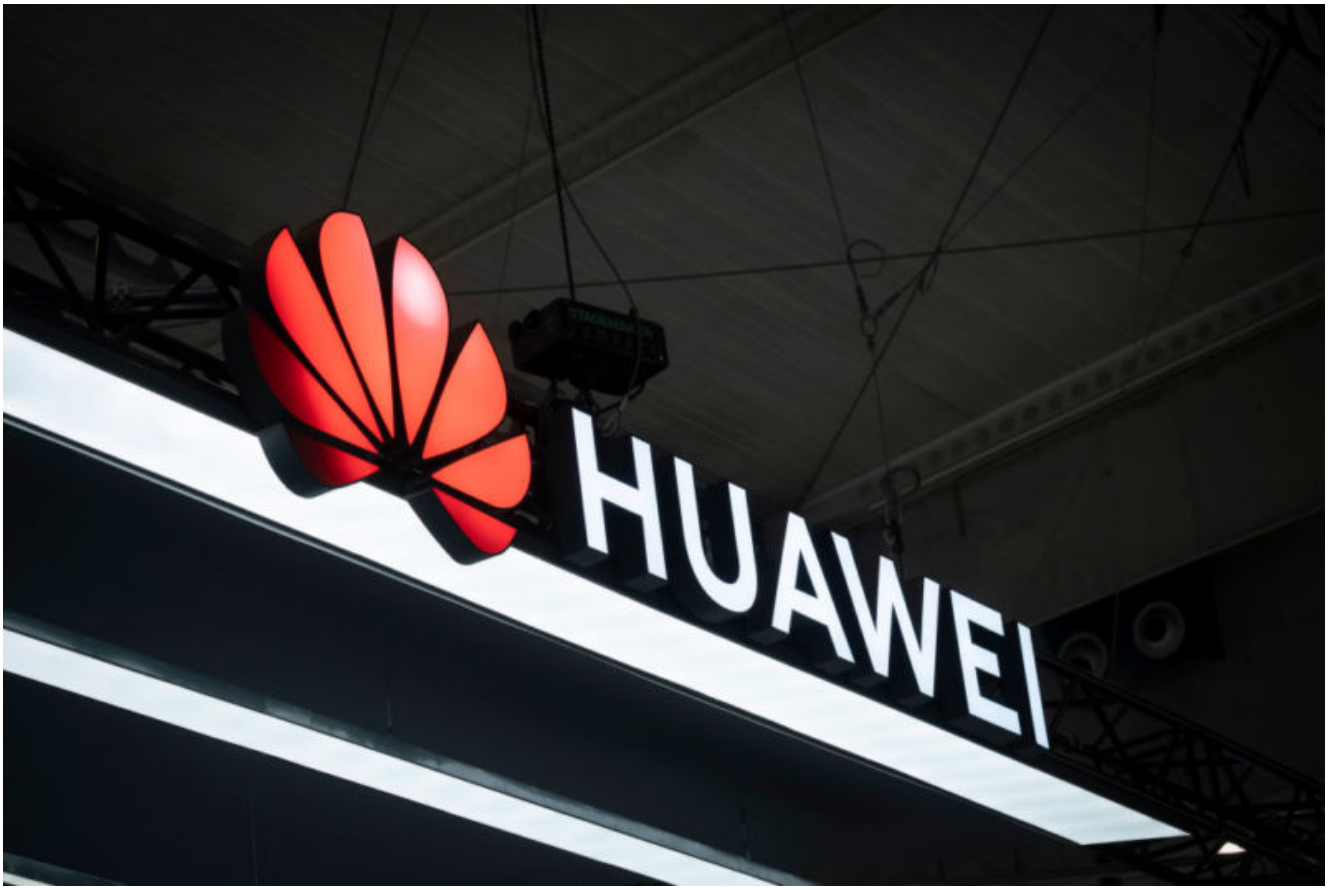
officials have cut from whole cloth this adjudicative agency-enforcement scheme," Oracle argued.

Oracle's suit is extremely unusual, Bloomberg Law reported today. While other companies have pushed back against rulings and data requests from this particular bureau, the Office of Federal Contract Compliance Programs (OFCCP), none has legally challenged its existence or authority in almost 40 years.

Legal experts who spoke to Bloomberg Law said there would be huge ramifications if Oracle were to win and the OFCCP "would cease to exist." That said, however, several experts Bloomberg interviewed seem to view that as unlikely, instead considering the suit a "Hail Mary" move, typical of the company.

https://arstechnica.com/?p=1628217

Huawei sues FCC to stop ban on Huawei gear in US-funded networks



Enlarge / Huawei’s logo at the Smart City Expo World Congress in Barcelona in November 2019.
Getty Images | SOPA Images

reader comments

108 with 51 posters participating

Share this story

Trade War! USA v. China

View more stories

Huawei has sued the Federal Communications Commission over the agency’s order that bans Huawei equipment in certain government-funded telecom projects.

“Huawei asks the court to hold the FCC’s order unlawful on the grounds that it fails to offer Huawei required due process protections in labelling Huawei as a national security

threat," the Chinese company said in a press release announcing the lawsuit. "Huawei believes that the FCC also fails to substantiate its arbitrary findings with evidence or sound reasoning or analysis, in violation of the US Constitution, the Administrative Procedure Act, and other laws."

Huawei said it filed the complaint in the US Court of Appeals for the Fifth Circuit. We haven't been able to get a copy of the lawsuit yet.

The FCC voted unanimously on November 22 to ban Huawei and ZTE equipment in projects paid for by the commission's Universal Service Fund (USF). The order will affect many small telecom providers that rely on the companies' network gear.

FCC Chairman Ajit Pai said at the time that Huawei and ZTE were chosen as ban targets because they "have close ties to China's Communist government and military apparatus. Both companies are subject to Chinese laws broadly obligating them to cooperate with any request from the country's intelligence services and to keep those requests secret. Both companies have engaged in conduct like intellectual property theft, bribery, and corruption."

Huawei contended that "Pai and other FCC commissioners failed to present any evidence to prove their claim that Huawei constitutes a security threat and ignored the facts and objections raised by Huawei and rural carriers after the FCC first made the proposal in March 2018."

Huawei accuses FCC of spreading fear

"These politicians ignore an important fact: Huawei has been working with rural US carriers for many years, and our customers trust our equipment," Huawei Chief Legal Officer

Song Liuping said, according to a transcript posted by Huawei. “They are experts in the security of their own networks, and they like working with us.”

Pai has “tried to spread fear about Huawei” by “us[ing] words like ‘backdoors’ to scare people. But they offer no proof,” Song said.

Song argued that carriers affected by the ban will end up using equipment from Nokia and Ericcson, which aren’t Chinese companies but do “manufacture in China.”

“The US government has never presented real evidence to show that Huawei is a national security threat,” Song said. “That’s because this evidence does not exist. When pushed for facts, they respond that ‘disclosing evidence might also undermine US national security.’ This is complete nonsense.”

Glen Nager, Huawei’s outside counsel, argued that the Huawei/ZTE ban “exceeds the FCC’s statutory authority” because “nothing in the Universal Service provisions of the Communications Act authorizes the Commission to make national security judgments or to restrict use of USF funds based on such judgments.”

The FCC ban will take effect upon being published in the Federal Register and will initially affect future projects paid for by the USF and the use of federal funding to maintain existing equipment. The FCC is also taking public comment on another plan to require removal of Huawei and ZTE equipment from networks that have already been built, and the commission is “seek[ing] comment on how to pay for such removal and replacement.”

Ban will cost small ISPs, Huawei

says

Huawei spokesperson Karl Song said that requiring the removal of equipment “would cost hundreds of millions of dollars” for small providers.

“We’ve built networks in places where other vendors would not go. They were too remote, or the terrain was difficult, or there just wasn’t a big enough population,” he said. “In the US, we sell equipment to 40 small wireless and wireline operators. They connect schools, hospitals, farms, homes, community colleges, and emergency services.”

Hoftstra University law professor Julian Ku said that “even a small [Huawei] victory in the case, one that makes the FCC go and start the process over again, would be a huge victory for them,” according to The New York Times. But it may be a difficult case for Huawei to win because US courts usually give federal agencies “a tremendous amount of deference,” Ku said.

https://arstechnica.com/?p=1628309

FCC tries to bury finding that Verizon and T-Mobile exaggerated 4G coverage



Enlarge / Ajit Pai, chairman of the Federal Communications Commission, during an interview in New York, on Tuesday, Nov. 5, 2019.

reader comments

16 with 16 posters participating

Share this story

Verizon, T-Mobile, and US Cellular exaggerated their 4G coverage in official filings to the Federal Communications Commission, an FCC investigation found. But FCC officials confirmed that Chairman Ajit Pai does not plan to punish the three carriers in any way. Instead, the FCC intends to issue an enforcement advisory to the broader industry, reminding carriers "of the penalties associated with filings that violate federal law."

"Overstating mobile broadband coverage misleads the public and can misallocate our limited universal service funds, and thus

it must be met with meaningful consequences," FCC staff said in an investigative report released today.

But there won't be any meaningful consequences for Verizon, T-Mobile, and US Cellular. "Based upon the totality of the circumstances, the investigation did not find a sufficiently clear violation of the MF-II [Mobility Fund Phase II] data collection requirements that warranted enforcement action," an FCC spokesperson told Ars via email.

In a call with reporters, a senior FCC official said that commission staff was unable to determine whether the carriers' exaggerations were deliberate. The official said that the investigation did not establish a clear violation of a specific rule. The FCC official said that maps submitted by carriers were based on industry-standard propagation models and that the FCC's own tests made it clear that those industry models do not reflect on-the-ground experience.

FCC officials conducted drive tests to determine whether the providers' reported coverage matched reality. The FCC staff report said:

> *Only 62.3 percent of staff drive tests achieved at least the minimum download speed predicted by the coverage maps—with US Cellular achieving that speed in only 45.0 percent of such tests, T-Mobile in 63.2 percent of tests, and Verizon in 64.3 percent of tests. Similarly, staff stationary tests showed that each provider achieved sufficient download speeds meeting the minimum cell edge probability in fewer than half of all test locations (20 of 42 locations). In addition, staff was unable to obtain any 4G LTE signal for 38 percent of drive tests on US Cellular's network, 21.3 percent of drive tests on T-Mobile's network, and 16.2 percent of drive tests on Verizon's network, despite each provider reporting coverage in the relevant area.*

FCC buries news

The FCC in 2017 required carriers to file maps and data indicating their 4G LTE coverage in order to help the commission determine which rural areas should get $4.5 billion in Mobility Fund money over 10 years. But small, rural carriers pointed out that big carriers exaggerated their coverage, potentially preventing those small carriers from getting funding to improve connectivity in areas that lack good service. The small carriers' complaints triggered an FCC investigation in December 2018.

The FCC's announcement of that investigation's findings today came in an odd manner that seemed designed to minimize the amount of attention it gets. A finding that some of the biggest wireless carriers in the US exaggerated mobile broadband coverage is certainly important enough to be mentioned in the headline of an FCC announcement.

Instead, Pai's office announced the issuance of the investigative report in the third paragraph of a press release titled, "Chairman Pai announces plan to launch $9 billion 5G fund for rural America." Pai's press release referred generally to carriers overstating coverage, but it did not name any of the specific carriers that did so.

Pai's office also held a press call with reporters in which FCC officials focused almost entirely on the new 5G fund rather than the carriers' inaccurate filings. As a result, early news coverage of the announcement focused more on the 5G fund than on the carriers' misdeeds.

The two announcements are related, as the FCC said it will try to improve the accuracy of data collection for the 5G fund, which will replace the old Mobility Fund plan. The 5G fund will supply $9 billion to carriers over 10 years, while the Mobility Fund would have distributed $4.5 billion over 10 years for 4G coverage. The money comes from the Universal

Service Fund, which is paid for by Americans through fees on their phone bills.

New data-collection system recommended

FCC officials didn’t voluntarily bring up the topic of whether Verizon, T-Mobile, and US Cellular will be punished for exaggerating coverage. But FCC officials confirmed that Pai does not intend to take enforcement action in response to a question from a reporter during the press call and in response to a question from Ars via email.

But Pai does agree with all of the recommendations FCC staff made in its report, including the recommendation to issue an enforcement advisory to the industry, a senior FCC official said. While the FCC said it found no evidence of a violation of Mobility Fund rules, the commission has yet to determine whether carriers violated rules in the separate Form 477 data-collection program.

FCC staff recommended the following:

> *[T]he Commission should analyze and verify the technical mapping data submitted in the most recent Form 477 filings of Verizon, US Cellular, and T-Mobile to determine whether they meet the Form 477 requirements. Staff recommends that the Commission assemble a team with the requisite expertise and resources to audit the accuracy of mobile broadband coverage maps submitted to the Commission. The Commission should further consider seeking appropriations from Congress to carry out drive testing, as appropriate. While Form 477 currently affords providers significant discretion in determining the extent of their mobile broadband coverage, this discretion does not encompass reporting inaccurate mobile coverage across extended areas in which consumers cannot receive any wireless signal whatsoever.*

FCC staff also recommended that the commission terminate the "challenge process" that resulted in small carriers pointing out errors in big carriers' maps.

"The MF-II coverage maps submitted by several providers are not a sufficiently reliable or accurate basis upon which to complete the challenge process as it was designed. The MF-II Challenge Process was designed to resolve coverage disputes regarding generally reliable maps; it was not designed to correct generally overstated coverage maps," the staff report said.

The FCC should come up with a better system to replace the challenge process, FCC staff said:

> *Mobile broadband coverage data specifications should include, among other parameters, minimum reference signal received power (RSRP) and/or minimum downlink and uplink speeds, standard cell loading factors and cell edge coverage probabilities, maximum terrain and clutter bin sizes, and standard fading statistics. Providers should be required to submit actual on-the-ground evidence of network performance (e.g., speed test measurement samplings, including targeted drive test and stationary test data) that validate the propagation model used to generate the coverage maps. The Commission should consider requiring that providers assume the minimum values for any additional parameters that would be necessary to accurately determine the area where a handset should achieve download and upload speeds no less than the minimum throughput requirement for any modeling that includes such a requirement.*

Exaggerated coverage has been a problem both for mobile and home broadband, as Form 477 rules have long allowed each ISP to count an entire census block as served even if it can serve just one home in the block. The FCC voted in August to finally collect more accurate data, with a new requirement that home

Internet providers give the FCC geospatial maps of where they provide service instead of merely reporting which census blocks they offer service in.

https://arstechnica.com/?p=1627939

New Iranian wiper discovered in attacks on Middle Eastern companies



reader comments

6 with 5 posters participating

Share this story

IBM X-Force, the company’s security unit, has published a

report of a new form of “wiper” malware connected to threat groups in Iran and used in a destructive attack against companies in the Middle East. The sample was discovered in a response to an attack on what an IBM spokesperson described as “a new environment in the [Middle East]—not in Saudi Arabia, but another regional rival of Iran.”

Dubbed ZeroCleare, the malware is “a likely collaboration between Iranian state-sponsored groups,” according to a report by IBM X-Force researchers. The attacks were targeted against specific organizations and used brute-force password attacks to gain access to network resources. The initial phase of the attacks was launched from Amsterdam IP addresses owned by a group tied to what IBM refers to as the “ITG13 Group”—also known as “Oilrig” and APT34. Another Iranian threat group may have used the same addresses to access accounts prior to the wiper campaign.

“While X-Force IRIS cannot attribute the activity observed during the destructive phase of the ZeroCleare campaign,” the researchers noted, “we assess that high-level similarities with other Iranian threat actors, including the reliance on ASPX web shells and compromised VPN accounts, the link to ITG13 activity, and the attack aligning with Iranian objectives in the region, make it likely this attack was executed by one or more Iranian threat groups.”

In addition to brute force attacks on network accounts, the attackers exploited a SharePoint vulnerability to drop web shells on a SharePoint server. These included China Chopper, Tunna, and another Active Server Pages-based webshell named “extensions.aspx,” which “shared similarities with the ITG13 tool known as TWOFACE/SEASHARPEE,” the IBM researchers reported. They also attempted to install TeamViewer remote access software and used a modified version of the Mimikatz credential-stealing tool—obfuscated to hide its intent—to steal more network credentials off the compromised servers. From there, they moved out across the network to spread the

ZeroCleare malware.

Hiding the driver

ZeroCleare, like the Shamoon wiper, uses the legitimate RawDisk software driver from EldoS to gain direct access to disk drives and write data. Since the EldoS driver is not signed, however, ZeroCleare uses a vulnerable but signed driver from a version of Oracle's VirtualBox virtual machine software to bypass signature checking of the driver—allowing it to attack 64-bit versions of Windows. The VBoxDrv driver, which passes Microsoft's Driver Signature enforcement, is loaded by an intermediary executable—in the IBM X-Force detected cases, the file was named **soy.exe**. After loading the vulnerable VirtualBox driver, the malware exploits a bug in the driver to load the unsigned EldoS driver. On 32-bit Windows systems, which lack Driver Signature Enforcement, the malware can dispense with the workaround and run the EldoS driver directly.

The payload of the malware is called ClientUpdate.exe. Using the EldoS driver, it overwrites the Master Boot Record and disk partitions of the infected machine.

The victims in the attacks were in the energy and industrial sectors in countries that Iran sees as rivals in the Persian Gulf. And this isn't the only ongoing Iran-tied campaign—there have been anecdotal reports of other attacks from Iran's APT33 against US and other nations' energy companies, and another Iranian-tied threat group targeted a US presidential campaign (President Trump's, according to Reuters).

https://arstechnica.com/?p=1627811

Mobile industry has stifled eSIM—and the DOJ is demanding change



reader comments

6 with 6 posters participating

Share this story

The US Department of Justice has given its tentative approval to a wireless-industry plan to revise eSIM standards, saying that new safeguards should prevent carriers from colluding against competitors in the standards-setting process. But the DOJ warned the industry that it must eliminate anti-competitive provisions from the current eSIM standard or face possible antitrust enforcement.

The DOJ last year began investigating AT&T, Verizon, and the GSMA, a trade group that represents mobile carriers worldwide. The antitrust enforcer found that incumbent carriers stacked the deck against competitors while developing an industry standard for eSIM, the embedded SIM technology that is used instead of removable SIM cards in new smartphones and other devices.

In theory, eSIM technology should make it easier to switch carriers or use multiple carriers because the technology doesn’t require swapping between physical SIM cards. But how it works in practice depends heavily on whether big carriers dominate the standard-setting process.

The DOJ investigation found that “the GSMA and its mobile network operator members used an unbalanced standard-setting process, with procedures that stacked the deck in their favor, to enact an RSP (Remote SIM Provisioning) Specification that included provisions designed to limit competition among networks,” the agency said last week.

That flawed process resulted in RSPv2, which makes it easy for a carrier to lock eSIM-equipped smartphones to its network, the DOJ said. The standard has so-called “profile policy rules” that require smartphones to “contain the capability for operator-controlled locking in order to be considered compliant with the RSP Specification,” the DOJ said. These provisions “may restrict the pro-competitive potential of eSIMs without being necessary to achieve remote provisioning or to solve an interoperability problem,” the DOJ said.

The current standard also has provisions that make it harder for phones to automatically switch between networks when the phone “detects stronger network coverage or a lower-cost network,” the DOJ said. The standard also “prevents an eSIM from actively using profiles from multiple carriers simultaneously.”

DOJ will watch and wait

Despite that, the DOJ said it won't file an antitrust lawsuit. That's because the GSMA agreed to a new standard-setting process that addressed DOJ concerns and will use that process to develop a new standard that will replace RSPv2. The DOJ said it is satisfied by the GSMA's process changes but that it will monitor the implementation of the new standard and may take action if the GSMA doesn't remove anti-competitive provisions in the next version of RSP.

The GSMA described its new process—called AA.35—in a letter to the DOJ in July, and DOJ antitrust chief Makan Delrahim provided an update on the agency's "present enforcement intentions regarding GSMA's proposal" in a letter to the GSMA last week. The DOJ said it "presently has no intention to challenge AA.35, if it goes into effect," because the new process "includes sufficient protections to minimize the chances of anticompetitive self-dealing inside the GSMA if it is applied as contemplated."

However, the DOJ said it "will closely observe how AA.35 is applied and whether it succeeds in promoting interoperability." The DOJ also warned the GSMA that if carriers form separate agreements to limit competition, "such agreements are always subject to independent antitrust scrutiny."

What the industry agreed to

Originally, the GSMA let non-carriers such as smartphone manufacturers participate in the standard-development process but made sure that all final decisions were controlled by mobile carriers. The DOJ said it was "concerned that the GSMA's operator-dominated process was used with the purpose and effect of altering what would otherwise have been competitive negotiations between the operators and smartphone

manufacturers (‘OEMs’) over the design and implementation of eSIMs.”

But after the DOJ began investigating, the GSMA came up with the alternative AA.35 process. As the DOJ noted, “AA.35 creates a two-stage process, with an Industry Specification Issuing Group (‘ISIG’) that creates the standards and an Industry Specification Approving Group (‘ISAG’) that approves the standards.”

ISIG membership is open “to all members, ensuring that there will not be operator-exclusive committees driving the process,” the DOJ continued. Non-carriers can become members of the ISAG, which “eliminates the complete control that operators previously had and instead gives all parts of the industry an opportunity to be represented,” the DOJ said.

Another safeguard prevents standards from being approved without the consent of smartphone makers. “At the ISAG level, [AA.35] requires approval of standards by separate majorities of the ISAG operator- and non-operator members,” the DOJ said. “Both bodies require an explanation of negative votes, another improvement that increases transparency and indicates meaningful attempts to reach consensus.”

Another new provision allows for appeals to be heard by an independent panel. Finally, operators can’t bypass or change this process “without the support of non-operator members” because the dual-majority voting structure requires consent of both groups, the DOJ said.

Getting rid of anti-competitive provisions

The current version of the eSIM standard, which was passed under the old, flawed process, has “several key features that have restricted the disruptive potential of eSIMs to date,”

the DOJ said. That’s a reference to the phone-locking provision described earlier in this article and “provisions that restrict the number of active profiles on an eSIM or impede the user’s ability to consent to dynamic profile switching,” the DOJ said.

For example, RSPv2 requires consumers to give their approval each time an eSIM “toggles between profiles or networks,” preventing the scenario where a phone automatically switches between networks “if it detects stronger network coverage or a lower-cost network,” the DOJ said.

A RSPv2 prohibition on using profiles from multiple carriers simultaneously could prevent scenarios where users have their phone divided into work-related and personal profiles or multiple “profiles optimized for different coverage areas or for international travel,” the DOJ said. Incumbent carriers apparently wanted that restriction to undercut “a potential competitive threat [that] would allow a user to divide usage across operators,” the DOJ said.

When the GSMA uses its new AA.35 process to create a new standard, the DOJ said it expects the group to reconsider those anti-competitive rules.

“The Department will take a special interest in whether RSPv3 includes provisions that are motivated only by the incumbent operators’ interest in gaining a competitive advantage or stifling new sources of competition,” Delrahim warned the GSMA. The DOJ “reserves the right to bring an enforcement action in the future” if the GSMA’s implementation of AA.35 “proves to be anticompetitive in purpose or effect,” he wrote.

https://arstechnica.com/?p=1627231