FCC: TracFone made up “fictitious” customers to defraud low-income program

Getty Images | Jozef Polc | 500px

reader comments

31 with 31 posters participating

Share this story

TracFone Wireless is facing a potential $6 million fine for allegedly defrauding a government program that provides discount telecom service to poor people.

The Federal Communications Commission proposed the fine against TracFone yesterday, saying the prepaid wireless provider obtained FCC Lifeline funding by “enroll[ing] fictitious subscriber accounts.” TracFone improperly sought and received more than $1 million from Lifeline, the FCC said.

The FCC press release said:

> *TracFone’s sales agents—who were apparently compensated via commissions for new enrollments—apparently manipulated the eligibility information of existing subscribers to create and enroll fictitious subscriber accounts. For example, TracFone claimed support for seven customers in Florida at different addresses using the same name, all seven of whom had birth dates in July 1978 and shared the same last four Social Security Number digits. The Enforcement Bureau’s investigation also found that, in 2018, TracFone apparently sought reimbursement for thousands of ineligible subscribers*

> *in Texas.*
>
> *Today's proposed fine is based on the 5,738 apparently improper claims for funding that TracFone made in June 2018 and includes an upward adjustment in light of the company's egregious conduct in Florida.*

The FCC's Lifeline program, which is paid for by Americans through fees imposed on phone bills, provides monthly subsidies of up to $9.25 per household for phone and broadband service provided to eligible low-income subscribers.

FCC Chairman Ajit Pai said the commission "will not sit idly by and let Lifeline carriers fabricate enrollment data to generate more sales." Pai also said he is "hopeful that our new rule prohibiting carriers from paying commissions to employees or sales agents based on the number of Lifeline customers they sign up will help deter the kind of apparent fraud we've seen in this case."

The $6 million fine was proposed in a Notice of Apparent Liability for Forfeiture (NAL). TracFone will be given a chance to respond to the FCC's allegations in an effort to reduce or eliminate the proposed fine. The process could lead to a settlement or the FCC voting to impose a final punishment without TracFone's agreement. The FCC has a poor record collecting on its proposed fines.

TracFone said it would respond "at the appropriate time" and that "we take seriously our stewardship of public dollars and will continue to focus on connecting millions of low-income customers to school, jobs, healthcare, and essential social services," according to Reuters.

TracFone returned $1.2 million

According to the NAL, "TracFone admitted that its sales agents had improperly enrolled … subscribers in Florida into the

Lifeline program."

In Florida, after allegations by the Universal Service Administrative Company (USAC), which administers Lifeline on behalf of the FCC, TracFone investigated internally and "discovered that several agents had found a way to misuse Lifeline enrollees' dependents' information to populate other enrollment applications." The NAL continued:

> *These agents apparently altered portions of the dependents' beneficiary data, such as individual digits in dates of birth or Social Security numbers. The agents apparently used the dependents' identifying information to enroll multiple members of the same household to generate additional sales. And TracFone apparently compensated its Lifeline sales agents during the relevant time period by paying a commission on new enrollments. Thus, the agents apparently earned money by fabricating the new enrollments and TracFone benefited by receiving Lifeline support by submitting claims for them.*

The USAC also found that "TracFone had received federal Lifeline payments for thousands more Texas subscribers per month in 2018 than had been approved by" the state's Low-Income Discount Administrator (LIDA). In a seven-month period that began in June 2018, "TracFone apparently made 24,809 claims for Lifeline support… without first obtaining either (1) proper income-eligibility determinations from Texas or (2) proper program-based eligibility determinations from Texas," the FCC said.

TracFone already returned $1.2 million to the USAC for Lifeline money it received in Texas. The FCC said that "TracFone does not dispute that it made these claims for support" in its previous responses to the investigation. "Instead, TracFone contends that it did not knowingly seek reimbursement for customers in excess of those authorized by Texas."

The FCC said it rejected this defense "because TracFone willfully submitted the claims while certifying that all such claims were for eligible subscribers—and it knew, or should have known, that submitting claims for more subscribers than on the end-of-month determinative list that LIDA transmitted to TracFone would violate federal law." The FCC has a new program for verifying Lifeline claims to prevent fraud, but it wasn't yet operational in Texas or Florida when the alleged violations occurred.

Democratic FCC commissioners supported the action against TracFone but also urged the FCC to expand Lifeline's ability to help low-income Americans, particularly during the pandemic. Pai has been criticized for plans to restrict Lifeline support and lost a court case centering on one of those plans.

"We need to abandon the FCC's cruel policy proposals to cut off and restrict Lifeline and instead see how we can modernize the program and extend its reach," FCC Commissioner Jessica Rosenworcel said.

https://arstechnica.com/?p=1665574

Leaked Amazon memo: Walkout leader "not smart or articulate"

Enlarge / Chris Smalls.

reader comments

151 with 96 posters participating, including story author

Share this story

Amazon was eager to make warehouse manager Chris Smalls the face of worker activism at the company, an internal memo shows. The memo was leaked to Vice, which published excerpts of the document on Thursday.

“He’s not smart, or articulate, and to the extent the press wants to focus on us versus him, we will be in a much stronger PR position than simply explaining for the umpteenth time how we’re trying to protect workers,” wrote David Zapolsky, Amazon’s general counsel. Zapolsky was summarizing discussions at a daily meeting of senior Amazon executives focused on the coronavirus crisis. Vice reports that Amazon CEO Jeff Bezos attended the meeting.

Smalls was a manager at an Amazon fulfillment center on Staten Island, New York. It’s one of Amazon’s largest facilities, with around 5,000 workers. On Monday, Smalls was one of a number of workers—Amazon says 15, organizers say 60—who walked off the job to protest what they saw as inadequate precautions for worker health.

The workers claimed Amazon had not been transparent about the number of coronavirus cases at the factory. They were demanding that Amazon shut down the facility for a deep cleaning and to take more precautions to protect worker health once the facility reopened. (Amazon says it has already “taken extreme measures to keep people safe.”)

“Make him the face of the entire

union/organizing movement”

Amazon fired Smalls the day of the walkout. Smalls said this was in retaliation for organizing the walkout. Amazon disputed that, telling Ars that Smalls had been fired for ignoring instructions to self-quarantine, with pay, after coming into contact with a coworker who tested positive for the coronavirus.

In a CNBC interview later the same day, Smalls said that prior to his firing, he had been coming to work off the clock to “be that bridge from my associates to management. I went there every day of the week to inform my people—that they didn’t do—that somebody tested positive that they directly came into contact with. So I brought my people into the general manager’s office every single morning to voice their concern and try to get the building closed and sanitized.”

“Amazon wants to make this about me, but whether Jeff Bezos likes it or not, this is about Amazon workers—and their families—everywhere,” Smalls wrote in a Thursday statement. “There are thousands of scared workers waiting for a real plan from Amazon so that its facilities do not become epicenters of the crisis.”

Amazon’s Zapolsky really did want to make the Staten Island dispute about Smalls.

“We should spend the first part of our response strongly laying out the case for why the organizer’s conduct was immoral, unacceptable, and arguably illegal, in detail, and only then follow with our usual talking points about worker safety,” Zapolsky wrote in the memo leaked to Vice. “Make him the most interesting part of the story, and if possible make him the face of the entire union/organizing movement.”

Amazon has long had an antagonistic attitude toward worker organizing.

“We are not anti-union, but we are not neutral either,” said a video distributed to managers of Amazon-owned Whole Foods in 2018. “We do not believe unions are in the best interest of our customers, our shareholders, or most importantly, our associates. Our business model is built upon speed, innovation, and customer obsession—things that are generally not associated with unions.”

Amazon is aiming to hire an additional 100,000 workers to deal with surging demand. In March, Amazon raised its minimum pay from $15 to $17 an hour and offered workers double their regular pay for overtime hours.

Amazon’s labor shortage, along with the logistical challenges and health risks created by the coronavirus crisis, could create fertile ground for worker organizing.

https://arstechnica.com/?p=1665546

T-Mobile, Sprint took a risk by finishing merger without Calif. approval

Enlarge / California tells T-Mobile and Sprint to halt merger.
Getty Images | Stefan Jackowski | EyeEm

reader comments

42 with 31 posters participating

Share this story

California state regulators are trying to hold up the T-Mobile/Sprint merger, saying the companies don't yet have approval to combine their operations in the state.

T-Mobile and Sprint announced yesterday that the merger is a done deal and that the two companies are now one. But while the companies had *almost* all approvals from government authorities, they have not yet gotten the expected approval from the California Public Utilities Commission (CPUC). The CPUC is scheduled to vote on the merger approval and related conditions on April 16.

In response to yesterday's T-Mobile/Sprint announcement, the CPUC issued a ruling that says the companies "shall not begin merger of their California operations until *after* the CPUC issues a final decision on the pending applications."

We contacted T-Mobile today about yesterday's CPUC ruling and will update this article if we get a response.

The state Public Utilities Code prevents companies from merging their California operations without approval, the CPUC order said. "Both Joint Applicants, T-Mobile and Sprint, have California subsidiaries that are public utility telephone corporations under state law, and subject to the jurisdiction of this agency. The merger of the companies' operations in California is therefore subject to CPUC approval," the order said.

But T-Mobile and Sprint argue that the CPUC does not have jurisdiction over wireless transactions and that the merger can be completed without the agency's approval. T-Mobile and Sprint previously received approval from the Federal Communications Commission and Department of Justice, and they defeated a lawsuit filed by California and other states that were trying to block the deal.

Regardless of the outcome at CPUC, the merger is happening. But the dispute between the companies and the Golden State could result in litigation and affect whether the state is able to impose conditions on the deal. T-Mobile claimed that some of CPUC's planned conditions are "practically impossible" and "unfair and discriminatory to T-Mobile vs our competitors."

T-Mobile warned investors that there is a "risk of litigation or regulatory actions" arising "from T-Mobile's consummation of the business combination during the pendency of the California Public Utility Commission's review of the business combination."

The legal arguments

Steve Blum of Tellus Venture Associates has been tracking the dispute, explaining that "T-Mobile and Sprint asked to withdraw their application for California Public Utilities Commission approval of the wireline elements of their merger agreement." Sprint told the state regulator that it "is no longer providing services in California as a regulated public utility" because it completed a years-long process of transitioning old phone systems to Voice over Internet Protocol, which isn't regulated in the same way. Sprint said it is thus relinquishing the Certificate of Public Convenience and Necessity that it previously received from CPUC.

Sprint's wireline services are exclusively for enterprise and carrier customers, and not for residential users.

The California utility regulator's jurisdiction over the transfer of wireline operations is clear, but "the CPUC's authority over a mobile carrier is murky at best," as "mobile licenses are issued by the Federal Communications Commission, which approved the transfer," Blum wrote.

To support its jurisdiction, the CPUC says that "wireless

carriers are ‘telephone corporations’ and therefore public utilities under Public Utilities Code Sections 216, 233 and 234.” Although the CPUC acknowledges that states cannot regulate wireless rates, it says that states “retain jurisdiction over ‘other terms and conditions’ of wireless service.”

Back and forth

T-Mobile told the CPUC in a letter Tuesday that the agency “lacks jurisdiction over this transaction.” T-Mobile and Sprint also said they can’t wait any longer because the pandemic “has created unprecedented uncertainty and risk in the financial markets,” and “there are no assurances that the banks will continue to be able to fund the transaction if the closing is delayed any further.”

T-Mobile and Sprint expanded on their objections to the CPUC’s jurisdiction and proposed conditions in a longer filing. The CPUC’s proposed 5G build-out requirements go beyond FCC conditions, the companies said. Another CPUC-proposed requirement that the companies “shall offer in-home broadband service wherever 5G service is available” is “incompatible” with T-Mobile’s “un-refuted testimony that in-home broadband would be provided only where there is sufficient network capacity (sometimes referred to as ‘excess’ capacity),” the filing said.

T-Mobile and Sprint also objected to proposed requirements that it “maintain LTE speeds and coverage areas in California” until the 4G LTE network is decommissioned and to proposed 72-hour backup power requirements. They also objected to requirements to add 1,000 full-time jobs in California and to expand discount-service availability for low-income people.

https://arstechnica.com/?p=1665407

America’s COVID-19 testing has stalled, and that’s a big problem

Enlarge / After growing exponentially for most of March, US testing has stalled out at around 100,000 tests per day.
Eric Bangeman / Ars Technica

reader comments

148 with 77 posters participating, including story author

Share this story

One of America’s biggest fumbles in the early weeks of the coronavirus crisis was inadequate testing. Thanks to a series of poor decisions by federal officials, the United States had far too little capacity to test for COVID-19 throughout the month of February, hampering our ability to contain the spread of the virus.

In early March, things seemed to be turning around. According to data from COVID Tracking Project, daily testing grew exponentially from a few hundred tests on March 5 to 107,000 tests last Friday, March 27.

But since then, progress has stalled. The US has been testing a bit over 100,000 people a day for the last six days—including 101,000 yesterday. And that’s a cause for concern because the US will need to do considerably more testing to get its coronavirus outbreak under control.

Why testing matters

The most urgent need for testing is when a patient shows up at the hospital with coronavirus symptoms. Knowing if a patient actually has coronavirus or some other disease with similar symptoms determines what kinds of treatment are most appropriate. It also lets health care workers know whether they need to take precautions to avoid catching the coronavirus themselves.

Testing is also crucial for slowing the spread of coronavirus in the wider world. Ideally, when a patient is diagnosed with COVID-19, health officials would test everyone who has had close contact with that person. If someone else tested positive, officials would test all of *their* close contacts too. This process is known as contact tracing. Doing it on a wide-enough scale should allow officials to quickly identify and isolate almost everyone who has the disease.

You might not think that would matter now with so many people staying at home. But there are a fair number of people still working in essential industries who are at risk for catching COVID-19.

Amazon, for example, has had coronavirus cases at a growing number of fulfillment centers around the country. When these outbreaks occur, Amazon typically orders co-workers known to have had close contact to self-quarantine for 14 days. But those workers aren’t necessarily tested. So if one of them passed COVID-19 on to someone else before their quarantine began, public officials wouldn’t find out.

When to go back to work

So greater testing capacity would help improve treatment of patients and limit the spread of the coronavirus today. And it will become even more important once the current outbreak has

peaked and public officials want to start sending people back to work.

If officials simply lifted quarantine restrictions without taking other precautions, the virus would resume its exponential growth and we'd wind up with a second large-scale outbreak. Aggressive contact tracing and quarantine policies are needed to make sure this doesn't happen. And that requires ample testing capacity.

Large-scale testing can also inform public officials' decision about when and how to lift restrictions. That's important because today's large-scale quarantine policy is having massive economic costs. The more data officials have about the spread of the coronavirus, the more precisely they can determine when and where it's safe to relax restrictions and the sooner they can let people go back to work.

Current testing levels aren't enough

The countries that have been most successful at controlling their coronavirus outbreaks have done a lot more testing than the United States on a per capita basis. South Korea, for example, has performed 431,000 tests since its outbreak began. On a per capita basis, that's equivalent to 2.7 million tests in the US. We've only done 1.1 million tests so far, according to the COVID Tracking Project.

South Korea's testing has actually leveled off at around 10,000 tests per day. But that's because South Korea has gotten its coronavirus outbreak under control. It's had 9,976 total infections, and it had only 89 new infections on Thursday. In contrast, the US has had more than 236,000 infections, with tens of thousands of new infections daily. That's far more than South Korea even after you adjust for population. So we're going to need much more testing to get

the situation under control.

Another example: Germany is conducting 50,000 tests per day. That's about twice as much testing as the US on a per capita basis. Germany's aggressive testing may have helped the country keep its coronavirus fatality rate low.

Governors in the United States say that a shortage of testing supplies is hampering their fight against the virus. The New York Times recently obtained audio of a call between governors and President Trump:

> *Gov. Steve Bullock of Montana, a Democrat, said that officials in his state were trying to do "contact tracing"—tracking down people who have come into contact with those who have tested positive—but that they were struggling because "we don't have adequate tests."*

"We have a desperate need for testing kits," Washington Gov. Jay Inslee told CNN on Sunday.

The rising rate of positive results is an ominous sign

When testing resources are scarce, health professionals prioritize testing people with obvious COVID-19 symptoms. If testing capacity were growing faster than coronavirus infections, we would expect more testing of people with milder symptoms or no symptoms at all. That should lead to a declining rate of positive test results.

Instead, the fraction of positive test results has been steadily rising over the last two weeks. The week of March 15, around 13 percent of coronavirus tests produced positive results, according to COVID Tracking Project data. Last week it was 17 percent. So far this week, 22 percent of coronavirus tests have produced positive results. Yesterday's figure was

more than 25 percent.

This doesn’t *necessarily* mean that the number of infections is growing faster than our testing capacity. For example, it’s possible that as health care workers have become more familiar with the virus they’ve gotten better at identifying probable coronavirus cases, allowing them to prioritize testing of people who are likely to have the virus.

But it does suggest that our testing capacity isn’t significantly outpacing the number of infections. And a 25 percent positive testing rate also suggests that we don’t currently have enough testing capacity to truly bring the virus under control, because thorough contact tracing is going to require testing a lot more than four people for every infection.

https://arstechnica.com/?p=1665191

$12.8 billion Juul investment broke the law, FTC suit says

Enlarge / A person holds a Juul Labs Inc. e-cigarette next to packages of flavored pods on Thursday, Dec. 20, 2018.

reader comments

26 with 23 posters participating, including story author

Share this story

Back in 2018, cigarette maker Altria—formerly known as Philip Morris— apparently saw the writing on the wall for the tobacco industry's future. In December of that year, the company dropped a cool $12.8 billion to gain a 35 percent minority stake in e-cigarette firm Juul. The Juul deal seemed like a particularly clever way to gain a massive toehold in the vaping market as traditional tobacco cigarette use waned—too clever, it seems, as now the Federal Trade Commission is suing to unwind the deal.

The transaction "eliminated competition in violation of federal antitrust laws," the FTC said yesterday, announcing the unanimous vote to move forward with the suit.

At the time of the acquisition, Juul was the leading US e-cigarette brand, the FTC alleges, but Altria's own MarkTen product was already the second most popular brand by market share. Instead of continuing to compete, however, Altria arranged to reap the benefits of its competitor without outright acquiring it.

"Altria orchestrated its exit from the e-cigarette market and became Juul's largest investor," Ian Conner, director of the FTC's bureau of competition, said. "Altria and Juul turned from competitors to collaborators by eliminating competition and sharing in Juul's profits."

Altria, for its part, intends to "vigorously defend" the deal. "We believe that our investment in Juul does not harm competition and that the FTC misunderstood the facts," Altria general counsel Murray Garnick said. "We are disappointed with the FTC's decision, believe we have a strong defense, and will vigorously defend our investment."

A beleaguered buy

Altria's rebranding in 2003 followed the massive "Big Tobacco" suits in the 1990s. Although the tobacco firms fought for decades over meeting some of the settlement terms they agreed to, the reputational damage the cigarette industry sustained in the opening years of the 21st century was both deep and broad.

While more than 40 percent of Americans were cigarette smokers in the 1960s, that figure had dropped to an all-time low of 13.7 percent by 2018. What we had instead, however, was a massive surge in e-cigarette use, or vaping. In 2017, about 11 percent of high school seniors reported using e-cigarette products containing nicotine. By 2018, that figure was 21 percent, and it rose to 25 percent last year.

Through 2019, however, Juul began to find itself in trouble with federal regulators. The Food and Drug Administration in September blasted Juul for allegedly advertising directly to students *in schools* without parental consent. A week later, the company pulled all its advertising and fired the CEO.

A whistleblower lawsuit and the tangle with regulators ended up hitting the company's bottom line as well. In October, along with its third-quarter results, Altria announced a $4.5 billion write-down on its Juul investment. The fourth quarter was no better: in January, Altria wrote down another $4.1 billion of its investment, estimating Juul's overall valuation to be about $12 billion—less than that 35 percent stake was worth a mere year earlier.

https://arstechnica.com/?p=1665187

FCC requires anti-robocall tech after “voluntary” plan didn’t work out [Updated]

reader comments

169 with 121 posters participating

Share this story

Update (April 1, 2020): The Federal Communications Commission voted unanimously to finalize the anti-robocall order on March 31, 2020, complying with instructions the commission received from Congress. The order “requires all originating and terminating voice service providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021, a deadline that is consistent with Congress’s direction in the recently-enacted TRACED Act,” the FCC said. As we wrote earlier, the FCC plans a one-year deadline extension for small phone providers. The FCC also voted to seek public comment on how “to promote caller ID authentication on voice networks that do not rely on IP technology,” meaning older landline networks.

Original story from March 6, 2020 follows: Phone companies would be required to deploy technology that prevents spoofing of Caller ID under a plan announced today by Federal Communications Commission Chairman Ajit Pai.

Pai framed it as his own decision, with his announcement saying the chairman “proposed a major step forward… to protect consumers against spoofed robocalls.” But in reality the FCC

was ordered by Congress and President Trump to implement this new rule. The requirement on the FCC was part of the TRACED Act that was signed into law in December 2019. Pai previously hoped that all carriers would deploy the technology voluntarily.

“I’m excited about the proposal I’m advancing today: requiring phone companies to adopt a caller ID authentication framework called STIR/SHAKEN,” Pai said in his announcement. “Widespread implementation will give American consumers a lot more peace of mind when they pick up the phone.” The FCC will vote on the measure at its March 31 meeting.

The STIR and SHAKEN protocols use digital certificates, based on public-key cryptography, to verify the accuracy of Caller ID. STIR/SHAKEN would work best if all phone companies adopt it because it can only verify Caller ID when both the sending carrier and receiving carrier have deployed the technology. Robocallers who spoof real numbers to hide their identities would get flagged by STIR/SHAKEN. Depending on how each carrier implements it, flagged calls could be passed on to consumers with a warning or be blocked entirely.

Carriers have already been adopting STIR/SHAKEN, but Pai said not all companies have done so. “Last year, I demanded that major phone companies voluntarily deploy STIR/SHAKEN, and a number of them did,” Pai said. “But it’s clear that FCC action is needed to spur across-the-board deployment of this important technology.”

STIR/SHAKEN can be used by mobile phone providers and home VoIP services, but landline providers have said they can’t deploy it on the older TDM services that run on traditional copper phone lines. That won’t change with the FCC action, as the underlying US law and Pai’s proposal only “require originating and terminating voice service providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks.”

The requirement would apply to big carriers by June 30, 2021 and to small and rural providers one year later. In addition to mobile providers, companies that offer IP-based phone service over cable or fiber lines would have to comply.

Robocalls from outside US a major problem

While STIR/SHAKEN might help reduce robocalls or slow their growth, it’s not enough on its own to solve the large and complicated robocall problem. For one thing, a lot of robocalls originate from overseas. The FCC recently sent letters to seven US-based voice providers “that accept foreign call traffic and terminate it to US consumers,” saying these companies’ services are “being used as a gateway into the United States for many apparently illegal robocalls that originate overseas.” In a related action, the Department of Justice sued two small companies that allegedly connected hundreds of millions of fraudulent robocalls from Indian call centers to US residents.

The new US law that ordered the FCC to require SHAKEN/STIR gave the FCC discretion on how to regulate calls from overseas. Congress told the FCC to “consider” how the commission can “establish obligations on international gateway providers that are the first point of entry for these calls into the United States, including potential requirements that such providers verify with the foreign originator the nature or purpose of calls before initiating service.” But it’s up to the FCC on whether to take further action on that point.

We asked Pai’s office if his plan will have any impact on spoofed calls that originate from overseas and will update this article if we get an answer. The full text of Pai’s plan hasn’t been released yet.

https://arstechnica.com/?p=1658723

Teardown of Huawei flagship phone finds US parts despite blacklisting

Enlarge / The Huawei P40 Pro.

reader comments

53 with 30 posters participating

Share this story

Huawei is still using components made by US companies in its newest flagship smartphone, a Financial Times teardown has found, despite the US all but blacklisting the Chinese telecoms equipment manufacturer.

On Thursday, Huawei launched its P40 smartphone—one of the first flagship devices the company has launched since Washington's introduction of sanctions last May that barred US companies from selling to the Chinese group unless specifically licensed to do so.

In the wake of the sanctions, Huawei, which the Trump administration accuses of spying for Beijing, has had to find ways of replacing its US components. Crucially, Google can no longer supply its Android mobile services platform to the Chinese company.

The FT took apart a Huawei P40 Pro phone as well as last year's P30, released just before US sanctions hit, for

comparison. The teardown was done by XYZone, a Shenzhen-based company that disassembles smartphones and identifies the suppliers of their components.

Phone makers sometimes use different components in different batches of the same smartphone, and the FT teardown was modeled on the earliest available copy of the P40.

The biggest surprise was that some parts from US companies were still ending up in the newest Huawei smartphone, despite the US all but banning its companies from selling to the Chinese tech company.

The P40’s radio-frequency front-end modules were, according to XYZone’s teardown analysis, produced by Qualcomm, Skyworks, and Qorvo, three US chip companies. RF front-end modules are

critical parts of the phone that are attached to the antennas and required to make calls and connect to the Internet.

The Qualcomm component is covered by a license from the US Commerce Department, according to a person familiar with the company. Qorvo and Skyworks did not respond to requests for comment.

“Huawei has shown resilience by replacing many US components over the course of a single phone-design cycle. Its continued use of Qorvo and Skyworks chips also shows that it’s too difficult to break dependence on US technology,” said Dan Wang, technology analyst at research firm Gavekal Dragonomics.

RF front-end modules are a form of analogue chip, a sector in which the United States still has dominance, Wang said. “As the US debates tightening sanctions on Huawei, the company’s resilience will be tested more severely in the coming year,” he added.

The RF front-end modules in last year’s P30 also came from Qualcomm, Skyworks, and Qorvo, whose stock prices plunged on news of US sanctions against Huawei.

The “Entity List” designation means that US companies have to apply for a license to export any US-origin technologies to Huawei. The US government has granted a “temporary general license” to its companies, allowing them to sell to Huawei to service existing products—helping clients such as telecoms carriers that may need to replace parts of their wireless equipment.

But the general license does not cover sales for the purpose of making new products, such as the P40 smartphone. For that, companies must seek individual licenses, and the Department of Commerce has not said which ones it has granted them to.

A spokesperson for Huawei said the company has “always complied with any export control regulations of various countries, including the United States” and that “all the product materials are obtained legally from our global partners, and we insist on working with our partners to provide consumers with high quality products and services.”

Other notable changes from last year include the potential disappearance of US chipmaker Micron from the P40 Pro—or at least from the batch that the FT received. Micron made the storage devices called NAND flash memory chips for some batches of last year’s P30 smartphone, and South Korea’s Samsung made the same chips for other batches. The FT’s copy of this year’s P40 Pro appears to have only Samsung NAND flash memory chips.

Both the P30 and the P40 are largely made of components manufactured and assembled by Chinese, South Korean, and Taiwanese companies, with only a small fraction of the overall value of components originating from US companies.

Yet US companies have historically held strategic chokepoints on Huawei’s phones, from the Android operating system to RF front-end chips and the chip architectures by Arm Holdings, which formed the basis of Huawei’s in-house chip design unit HiSilicon.

Huawei component sourcing

P30	**P40 Pro**	
Component	**Manufacturer (country)**	**Manufacturer (country)**
Read-only memory (NAND flash)	Micron (US) (some batches)/ Samsung (South Korea) (some batches, eg P30 Pro)	Samsung (South Korea)

Radio-frequency front-end modules	Qualcomm (US); Skyworks (US); Qorvo (US)	Skyworks (US); Qorvo (US); Qualcomm (US)
Communication and radio frequency chips	Qorvo (US)	Could not be identified
Near-field communication chips	NXP (Netherlands)	NXP (Netherlands)
Screen	Samsung (South Korea)	BoE (China); LG (South Korea)
Microprocessor (system on chip)	Huawei’s HiSilicon (China)	Huawei’s HiSilicon (China)
Battery	Desay (China); Amperex (China)	Desay (China); Amperex (China)
Lens	Sony (Japan)	Sony (Japan)

Additional reporting by Richard Waters in San Francisco.

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

https://arstechnica.com/?p=1664713

Authors fume as online library “lends” unlimited free books

Enlarge / Sign in front of Middle Country public Library in

Centereach, New York, on March 26, 2020.

reader comments

152 with 91 posters participating, including story author

Share this story

For almost a decade, the Internet Archive, an online library best known for its Internet Wayback Machine, has let users "borrow" scanned digital copies of books held in its warehouse. Until recently, users could only check out as many copies as the organization had physical copies. But last week, The Internet Archive announced it was eliminating that restriction, allowing an unlimited number of users to check out a book simultaneously. The Internet Archive calls this the National Emergency Library.

Initial media coverage of the service was strongly positive. The New Yorker declared it a "gift to readers everywhere." But as word of the new service spread, it triggered a backlash from authors and publishers.

"As a reminder, there is no author bailout, booksellers bailout, or publisher bailout," author Alexander Chee tweeted on Friday. "The Internet Archive's 'emergency' copyrights grab endangers many already in terrible danger."

"It is a tarted-up piracy site," wrote author James Gleick.

The Authors Guild, a leading authors' organization, wrote Friday that it was "appalled" by the Internet Archive's move. "We are shocked that the Internet Archive would use the COVID-19 epidemic as an excuse to push copyright law further out to the edges, and in doing so, harm authors, many of whom are already struggling," the group wrote.

The Association of American Publishers also blasted the project last Friday. "We are stunned by the Internet Archive's

aggressive, unlawful, and opportunistic attack on the rights of authors and publishers in the midst of the novel coronavirus pandemic," wrote the group, which represents dozens of publishers, including most of the largest ones in the United States.

The Internet Archive responds

Enlarge / Hazard tape blocks the book returns slot at a London library.

In a Monday blog post, the director of the emergency library project, Chris Freeland, wrote that the emergency library concept was inspired by the closure of libraries across the United States and around the world.

"Right now, today, there are 650 million books that tax-paying citizens [in the US] have paid to access that are sitting on shelves in closed libraries, inaccessible to them," Freeland wrote. "To meet this unprecedented need at a scale never before seen, we suspended waitlists on our lending collection."

The post includes a section addressing common questions about the emergency library. One question addressed in the post is "What is the legal basis for Internet Archive's digital lending during normal times?" Freeland touts the practice of controlled digital lending, which he argues is legal under copyright's fair use doctrine—though no court has ruled on the question so far.

But the post doesn't directly address the legality of the library's latest incarnation, which offers unlimited copies of in-copyright books. Freeland notes that users are limited to reading a book for two weeks (though they can renew it). And he notes that the courts have ruled that it's legal for libraries to scan books. But he doesn't explain how the service's current incarnation complies with copyright law.

When I asked Cornell copyright scholar James Grimmelmann about the legality of the program last week, he seemed skeptical.

"There is no specific pandemic exception" under copyright law, he said. Copyright's fair use exception is open-ended, so theoretically a judge could decide that the emergency circumstances of a pandemic justify the Internet Archive's action. But there are few examples of courts making such a big leap. At a minimum, the Internet Archive is taking a substantial legal risk.

The question is whether anyone will actually file a lawsuit. Authors and publishers would likely have a strong case. But lawsuits are expensive, and suing an online library distributing books in the middle of a pandemic could be a public relations nightmare.

https://arstechnica.com/?p=1664596

FDA approves the emergency use of chloroquine for COVID-19

Enlarge / Medical staff at the IHU Mediterranee Infection Institute in Marseille shows packets of a Nivaquine (tablets containing chloroquine) and Plaqueril (tablets containing hydroxychloroquine) on February 26, 2020,.

reader comments

143 with 68 posters participating

Share this story

On Saturday, the Food and Drug Administration issued an Emergency Use Authorization that will allow patients suffering from COVID-19 to be treated using drugs without clear evidence of the drugs' efficacy. The move comes after President Donald Trump has touted the drugs' potential several times on the basis of tiny, anecdotal trials. There have also been reports of hoarding of the drugs, which are needed by people with some autoimmune disorders.

Potential or hype?

The drugs in question are relatives of chloroquine, specifically chloroquine phosphate and hydroxychloroquine sulfate. Originally developed as an antimalarial, chloroquine has a variety of effects, including the ability to reduce immune activity. That has made it useful for the treatment of autoimmune disorders such as lupus and rheumatoid arthritis. Given its multiple effects, it's not surprising that the drug

also has a variety of side effects, the most significant probably being a slowing of the heart's rhythm that can potentially lead to fatal complications. (Technically, the drug extends the QT interval.)

What does any of this have to do with a coronavirus? As we discussed when exploring potential treatments for SARS-CoV-2, chloroquine can also alter the pH of the compartment in which some viruses are brought into the cell. This can interfere with the process of depositing the virus' genome inside the cell and thus block the virus' ability to reproduce. Experiments in cultured cells infected by SARS-CoV-2 indicated that chloroquine treatments can keep the virus from spreading within the culture.

But cultured cells are very different from the environments the drugs would encounter in the human body, and SARS-CoV-2 obviously behaves differently from earlier coronaviruses. So ideally, we would want evidence that it works in humans against the source of the current pandemic.

Unfortunately, all we have at present is anecdotal evidence. One small trial indicated that the drug was somewhat effective on its own, with its effectiveness enhanced by an antibiotic. But a recent perspective on the drugs' use noted that the trial had "serious methodological flaws," and follow-up work lacked any negative controls to compare with the treated group. There are also indications that the trial was rushed through peer review at a journal edited by one of its authors, who has been involved with research that contains fabricated data.

Meanwhile, a small study performed in China saw no indication that the drug was effective on its own. And it's not clear why an antibiotic, which normally targets bacteria, would enhance the effect of an antiviral treatment. Larger, properly controlled clinical trials are already in progress, but it may be months before they produce enough data for us to make

evidence-based decisions here.

Wait for evidence?

But the absence of any other known treatments for this highly infectious disease has led to a number of people latching on to the anecdotal reports about chloroquine drugs, most prominently including President Trump. This has led to a nationwide shortage as doctors and even dentists have handed out unjustified prescriptions or attempted to hoard the drugs for themselves.

This has made the drugs difficult to obtain for those who use them to treat immune disorders, raising the prospect that some of the people with those autoimmune disorders will need extensive care from our overstretched medical system. And at least two people attempting to self-medicate have ended up dead. As a result, some scientists have been harshly critical of Trump's promotion of the drug.

But now the FDA has stepped in. In a letter released on Saturday, the FDA's Chief Scientist, Denise Hinton, responded positively to a request from the Department of Health and Human Services to provide an Emergency Use Authorization for chloroquine-based drugs. According to the law that governs Emergency Use, authorizations can be made after the Secretary of Health and Human Services declares a public health emergency, which has already happened. At that point, the judgement about whether an authorization should be granted is "based on the totality of scientific evidence available to the secretary, including data from adequate and well-controlled clinical trials, if available, it is reasonable to believe that the product may be effective in diagnosing, treating, or preventing" the cause of the emergency.

Obviously, "reasonable to believe" can mean different things to different people. Hinton specifically refers to what she terms the "limited" studies mentioned above and notes that a

handful of other countries have recommended the use of chloroquine. For her, this constitutes “reasonable.” For others, it almost certainly will not, ensuring that the decision will be controversial.

Who gets it?

The perspective we linked to above recommends that any use of chloroquine attempt to prioritize availability for those in clinical trials, as well as those who need it to treat other conditions. The FDA’s Authorization will be specifically for those who cannot enroll in a clinical trial and will attempt to fulfill their needs using the Strategic National Stockpile, with distribution from there to regional health authorities. According to The Washington Post, two pharmaceutical giants have already agreed to supply the stockpile with additional doses. Use will be limited to hospitals, which should avoid issues with public hoarding, although the distribution of any materials to health care providers has been very chaotic in the United States.

The guidance to patients and doctors on the use of the drug emphasizes our uncertainty. “Chloroquine phosphate is experimental because we do not know if it works for COVID-19,” the guidance for patients notes, before going on to say that “There is limited information known about the safety and effectiveness (whether this will make you better) of using chloroquine phosphate for hospitalized patients with COVID-19.” Doctors are warned that [t]he optimal dosing and duration of treatment for COVID-19 is unknown” and instructed to carefully monitor heart activity for indications of problems caused by the drugs’ side effects.

Given that we probably have weeks to months to go before properly controlled clinical-trial data allows us to make conclusions about any drug’s effectiveness, it’s likely that chloroquine will remain the standard treatment for the peak of

several regional epidemics in the US. The one thing that this decision does ensure is that we'll have lots of anecdotal reports on its use to complicate the public's understanding of treatment options.

https://arstechnica.com/?p=1664652

Zoom's privacy problems are growing as platform explodes in popularity

Enlarge / Zoom's San Jose, Calif., headquarters looks like a lovely place to be socially distanced from.

reader comments

45 with 36 posters participating, including story author

Share this story

We have several more weeks, if not several more months, to go in this sudden era of Everything from Home. Work from home, school from home, funerals from home, church from home, happy hour from home—you name it, and we as a society are trying as best as we can to pull it off remotely. Tech use as a result is up all over, but arguably the biggest winner to date of the "Oh, crap, where's my webcam" age is videoconferencing platform Zoom.

Zoom's ease of use, feature base, and free service tier have

made it a go-to resource not only for all those office meetings that used to happen in conference rooms but also for teachers, religious services, and even governments. The widespread use, in turn, is shining a bright spotlight on Zoom's privacy and data-collection practices, which apparently leave much to be desired.

The challenge is particularly pronounced in the health care and education sectors: Zoom does offer specific enterprise-level packages—Zoom for Education and Zoom for Healthcare—that have compliance with privacy law (FERPA and HIPAA, respectively) baked in. Many users in those fields, however, may be on the free tier or using individual or other types of enterprise licenses that don't take these particular needs into consideration.

Growing (privacy) pains

Zoom's privacy policy began to draw widespread attention more than a week ago for provisions about its storage and use of customer data. At the time, the platform said it would collect, store, and share with advertisers data potentially including "the content contained in cloud recordings, and instant messages, files, whiteboards" shared on the platform. That included videos and transcripts.

Amid the scrutiny, Zoom this week made some changes to that policy. "Zoom does not sell customer content to anyone or use it for any advertising purposes," the company now says in bold, italic lettering—a welcome change, to be sure.

The privacy policy itself, though, seems to be only the tip of the iceberg. An investigation Vice Motherboard published Friday found the Zoom iOS app shared usage data with Facebook—even for users who do not have Facebook accounts. According to Motherboard, Zoom was sending Facebook data showing when the user opened the app, details about the device the app was used on, the time zone and city the user connected

from, information about the mobile network the user was connected through, and a unique advertiser number used for tracking a device between apps.

Following the report, Zoom updated the app on Friday to cut off the feature, saying, “We originally implemented the ‘Login with Facebook’ feature using the Facebook SDK in order to provide our users with another convenient way to access our platform. However, we were recently made aware that the Facebook SDK was collecting unnecessary device data.”

The company is still facing a lawsuit from a plaintiff in California, however. The suit (PDF), which seeks class-action status, alleges that Zoom violated the California Consumer Privacy Act (CCPA), which went into effect on January 1, arguing Zoom “failed to properly safeguard the personal information of the increasing millions of users of its software application.”

Worse, a feature meant to streamline connection for corporate users seems to be leaking some Zoom users’ personal contact information. A report today, also by Vice Motherboard, found that users who sign up from the same email domain are automatically being added to each others’ contact lists. For a workplace scenario, this makes sense: if two users both sign up using @arstechnica.com email addresses, odds are we work for the same employer and would need to talk to each other for work purposes. Businesses’ contacts get populated into Zoom this way regularly.

Users signing up with personal email addresses, however, are *also* having their information shared with other users of the same domain. One user shared with Motherboard a screenshot showing almost 1,000 other users—all strangers to him—listed in a “company directory.” Some widely used domains, including gmail.com, yahoo.com, and hotmail.com, are excluded from the company directory. Smaller domains used by individuals, though, appear not to be on the exclusion list.

Broken promises?

Zoom promises a bevy of protections for hosts who create meetings. At the top of that list is a promise that users can "secure a meeting with end-to-end encryption." That sounds pretty great! Unfortunately, it also might not be exactly true.

A report published today by The Intercept finds that the claim might be misleading. Instead of end-to-end encryption for audio and video, Zoom offers something slightly different, called transport encryption.

When The Intercept asked Zoom about its encryption capabilities, a spokesperson straight-up responded that they can't do it. "Currently, it is not possible to enable E2E encryption for Zoom video meetings," the spokesperson said, adding, "Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

If the data were truly encrypted end-to-end, only the users on either end of it would be able to access it. Under the TLS encryption it actually uses, though, Zoom itself could access the content that flows back and forth in meetings.

The company stressed to The Intercept that it does not, saying in a statement:

> *Zoom has layered safeguards in place to protect our users' privacy, which includes preventing anyone, including Zoom employees, from directly accessing any data that users share during meetings, including—but not limited to—the video, audio and chat content of those meetings. Importantly, Zoom does not mine user data or sell user data of any kind to anyone.*

If the data can be accessed, however, Zoom could be compelled to share it with government or law enforcement requests. Zoom, unlike many other technology and social media platforms, does not publish a transparency report regarding takedown and law enforcement requests it may have received.

All the reports, taken together, have drawn the attention of at least one legal authority: the office of New York Attorney General Letitia James is now investigating Zoom's privacy and security practices.

The New York Times obtained a letter from James' office to Zoom, which expressed concern "that Zoom's existing security practices might not be sufficient to adapt to the recent and sudden surge in both the volume and sensitivity of data being passed through its network." And while the company is responding quickly to specific vulnerabilities piecemeal as they become widely known through media reports, the attorney general's office "would like to understand whether Zoom has undertaken a broader review of its security practices."

"Zoom takes its users' privacy, security, and trust extremely seriously," the company said in a statement. "We appreciate the New York Attorney General's engagement on these issues and are happy to provide her with the requested information."

https://arstechnica.com/?p=1664495