Chip and phone supply chain shaken as Huawei faces mortal threat

Bloomberg | Getty Images

reader comments

169 with 88 posters participating

Share this story

Trade War! USA v. China

View more stories

The global chip and smartphone industries are bracing for severe disruption after the US launched tougher sanctions against Huawei that some said could mean “death” for the company.

Washington said on Monday that no company worldwide would be allowed to sell semiconductors made using US software or equipment without a license if Huawei was involved at any stage of the transaction.

The move closed a loophole in a May version of the rule that allowed Huawei to buy off-the-shelf chips if they were not custom-made to its designs.

Observers said given the dominance of US tools in certain segments of chipmaking, the new rule amounted to a blanket ban on any chip sales to Huawei, hitting its 5G equipment and

handset businesses.

“We believe this step to significantly (almost completely) curtail Huawei’s ability to source any semiconductor from anyone,” Manish Nigam, head of Asian technology research at Credit Suisse, said in a research note.

> *Huawei is probably finished as a maker of 5G network equipment and smartphones once its inventories run out early next year.*
> *Dan Wang, Gavekal Research*

The toughened US measures come as Huawei is vying for the title of the biggest handset maker on the planet and is trying to roll out its 5G networks around the world against opposition from Washington.

“Huawei is probably finished as a maker of 5G network equipment and smartphones once its inventories run out early next year,” said Dan Wang, of Gavekal Research in a report on the sanctions titled: “A Death Sentence For Huawei.”

“This now stops [US chipmakers] Nvidia, Intel, everyone, and they were not impacted before,” said an industry expert, adding that the tighter restrictions would affect billions of dollars in business across the sector.

Zhao Lijian, a spokesman for China’s foreign ministry, said on Tuesday that the new sanctions against Huawei were “undisguised bullying” and the US was “stretching the concept of national security and abusing state power.”

Analysts said MediaTek would probably be the first victim. The Taiwanese chip design house helped spawn generations of Chinese handset makers by offering off-the-shelf chip solutions. MediaTek’s shares dropped by almost 10 per cent in early trading on Tuesday, leading an Asia-wide plunge in semiconductor stocks.

After the initial Huawei chip restrictions in May, Huawei had

been planning to switch its smartphones from chips designed in-house to those from MediaTek to get around the ban.

“MediaTek will face an impact, though partially offset by its 38 percent share into other vendors,” Randy Abrams, an analyst at Credit Suisse, said in a research note. The bank downgraded the company to Neutral.

Analysts said the news would boost rival smartphone producers to Huawei.

“If Huawei cannot buy chipsets for its handsets, its handset business will probably disappear,” wrote Edison Lee at Jefferies.

He predicted that Oppo, Vivo, and Xiaomi would gain global market share. This would boost Qualcomm as the three rival Chinese brands relied more heavily on the US chip design house that competes with MediaTek.

However, some analysts said Washington’s tough move against Huawei could play out differently if Beijing hit back.

“Given such sanctions significantly impact Huawei, there could be retaliation from China,” said Sebastian Hou at CLSA. He named Apple, Huawei’s competitor in the smartphone market, and Qualcomm as potential targets.

South Korea’s computer chip manufacturers Samsung Electronics and SK Hynix, which supply memory chips to Huawei, were on Tuesday assessing the potential impact.

“Our understanding is that all chip supply, including memory chips, to Huawei will be subjected to the new US regulations,” said Sanjeev Rana, a Seoul-based tech sector analyst with CLSA. Samsung and SK Hynix declined to comment.

Analysts saw some possible upside from Huawei’s woes for Samsung’s mobile phone and 5G networks businesses. “We can expect the smartphone market to rebalance with Huawei’s market

share taken up by other smartphone [companies] and hence it would be neutral to the memory chip demand," Rana added.

Shares in Samsung edged higher in Seoul on Tuesday while SK Hynix dipped slightly.

Among Japanese companies, shares in Sony fell more than 1 per cent. Jefferies analyst Atul Goyal estimated that Huawei was Sony's biggest customer in image sensors after Apple, accounting for about 20 percent of its image sensor operating profits and revenue.

"Sony has already reduced image sensor output and… [is] already taking into account the Huawei impact in their forecast," Goyal said.

Longer-term, analysts expect Sony to recover some of the losses from Huawei by expanding sales to other Chinese smartphone makers, such as Vivo and Xiaomi.

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

https://arstechnica.com/?p=1699753

Secret Service buys location data that would otherwise need a warrant

Enlarge / Dozens of apps on your phone know where you are, whether you're home, at a doctor's appointment, at the

airport, or sitting still in a blank white room to pose artfully for a photo shoot.

reader comments

17 with 16 posters participating

Share this story

An increasing number of law enforcement agencies, including the US Secret Service, are simply buying their way into data that would ordinarily require a warrant, a new report has found, and at least one US senator wants to put a stop to it.

The Secret Service paid about $2 million in 2017-2018 to a firm called Babel Street to use its service Locate X, according to a document (PDF) Vice Motherboard obtained. The contract outlines what kind of content, training, and customer support Babel Street is required to provide to the Secret Service.

Locate X provides location data harvested and collated from a wide variety of other apps, tech site Protocol reported earlier this year. Users can “draw a digital fence around an address or area, pinpoint mobile devices that were within that area, and see where else those devices have traveled” in the past several months, Protocol explained.

Agencies under the Department of Homeland Security—including Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)—have purchased access to cellphone location activity for investigations, The Wall Street Journal reported in February. In June, the WSJ also reported that the IRS purchased access to location data through commercial databases.

Easier than a warrant

Private companies can gather up, buy, sell, and trade all kinds of sensitive user data more or less however they want, with very few limitations—and they do.

All kinds of mobile apps collect location data, both legitimately and illegitimately, and then sell it to data brokers. The data brokers then pass on is theoretically anonymized—but in practice, easily identifiable.

The New York Times in 2018 demonstrated in a multimedia feature how easy it is to follow an individual around her whole daily life using a snapshot obtained from just one data aggregation firm. "The database reviewed by The Times—a sample of information gathered in 2017 and held by one company—reveals people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day," the paper wrote at the time.

Apps are not the only ones collecting and selling that information. All four national mobile carriers—Verizon, AT&T, and the now-combined Sprint and T-Mobile—were caught selling customers' location data without consent in 2018 and 2019.

Law enforcement agencies are required to get a warrant to obtain an individual's mobile phone location data, the Supreme Court ruled in 2018. Investigators have several times sought warrants to gather information for all phones that travel within a certain boundary during a certain period of time, known as geofencing.

But there are currently no rules on the books preventing law enforcement from simply purchasing whatever information they want from the existing market. Sen. Ron Wyden (D-Ore.) told Vice that needs to change.

"It is clear that multiple federal agencies have turned to

purchasing Americans' data to buy their way around Americans' Fourth Amendment Rights," Wyden told Motherboard. "I'm drafting legislation to close this loophole, and ensure the Fourth Amendment isn't for sale."

https://arstechnica.com/?p=1699476

ISIS allegedly ran a COVID-19 PPE scam site

Enlarge / Uh, you didn't buy your mask at FaceMaskCenter.com, right?
Kilito Chan / Getty Images

reader comments

41 with 30 posters participating

Share this story

The COVID-19 pandemic, and millions of people desperate for scarce protective equipment like masks and Tyvek suits, has presented a bonanza for scammers. Now, according to the US Department of Justice, it seems that even ISIS has gotten in on the game.

In a series of civil and criminal complaints and forfeiture notices released this week, the Justice Department has revealed that it seized hundreds of bitcoin and ethereum accounts, millions of dollars, and four websites from known Islamic extremist groups that were using those accounts and

funds to support terrorist operations. Prosecutors say the forfeited crypto assets from the groups, which include ISIS, the al-Qassam Brigades, and al Qaeda, represent “the government’s largest-ever seizure of cryptocurrency in the terrorism context.” The cryptocurrency haul alone totals more than $1 million according to Chainalysis, a blockchain-focused firm whose tools were used in the investigation.

Among the jihadist fundraising efforts the DOJ has nixed, however, one stands out as particularly brazen. Court documents [PDF] detail how an ISIS agent allegedly ran a scam website for COVID-19 personal protective equipment, or PPE, known as FaceMaskCenter.com.

ISIS’ participation in the COVID-19 PPE scam industry is just part of a wave of fraud that has flooded the Internet since the COVID-19 pandemic began, says Mark Turnage, chief executive of DarkOwl, a security firm that’s tracked COVID-19 scams online for months. “We’ve seen a massive volume of illegitimate materials like PPE being sold and never delivered,” Turnage says. “The fact that ISIS decided to get into this business, too, isn’t really surprising. Everyone’s a capitalist. They’re leveraging the pandemic, too.”

According to one civil complaint, a confidential source linked an ISIS “facilitator” who used the alias Murat Cakar with the operation of FaceMaskCenter.com, as well as four Facebook accounts that advertised the site. Cakar is believed to be responsible for managing multiple ISIS hacking operations; the complaint alleges that he received $100,000 from Zoobia Shahnaz, an American woman who had planned to travel to Syria to join ISIS, and who pleaded guilty to material support of terrorism in 2018 after laundering ISIS funds with bitcoin.

FaceMaskCenter.com claimed to offer FDA-approved N95 face

masks, as well as a wide range of other PPE, including Tyvek suits, gloves, goggles, and thermometers. “FaceMaskCenter is the original online personal protective equipment supplier and was the first of its kind,” read the website, which now shows only a seizure notice from the DOJ, US Treasury, and Department of Homeland Security.

It’s not entirely clear to what degree FaceMaskCenter was an outright scam, or whether it merely sold substandard PPE. The civil complaint against FaceMaskCenter.com states the masks offered on the site, for instance, were produced by a Turkish company and did not meet FDA standards, as advertised. When an US customer contacted FaceMaskCenter asking to buy masks and other PPE for hospitals, nursing homes, and fire departments, the DOJ says a Syrian national based in Turkey responded with an offer of up to 100,000 masks, a number the complaint describes as unrealistic given the scarcity of masks during the global pandemic. It’s unclear whether any masks were actually delivered.

FaceMaskCenter also claimed to be run by “sanitary experts,” and to have been founded in 1996, when in fact the domain was registered in late February of 2020, according to court documents. “There are a lot of different red flags,” says DarkOwl’s Turnage. “You can usually test just from the date of the creation of the domain whether this is a legitimate supplier versus someone who is just trying to capitalize on the pandemic.”

Aside from that PPE site seizure, the DOJ says that the IRS, FBI, and DHS’s Homeland Security Investigations unit also dismantled funding operations for al Qaeda and the Izz ad-Din al-Qassam Brigades, the militant wing of Hamas. According to a blog post from blockchain forensics firm Chainalysis about the operation, agents seized a total of more than $1 million in cryptocurrency, largely from an unlicensed money services business allegedly run by a Turkish man named Mehmet Akti. Chainalysis further writes that al Qaeda also funneled its

cryptocurrency donations, solicited on the web and on Telegram, through BitcoinTransfer, a bitcoin exchange based in Idlib, Syria.

But ISIS appears to have been unique among the groups—at least based on the behavior captured in the indictment—in using a COVID-19 scam to raise money, rather than mere appeals for donations. The result is that desperate customers of FaceMaskCenter.com may not have just been stiffed on orders of life-saving equipment, but unknowingly contributed to violent extremism, too.

This story first appeared on wired.com.

https://arstechnica.com/?p=1699324

Charter can charge online video sites for network connections, court rules

Enlarge / A Charter Spectrum van in West Lake Hills, Texas, in April 2019.

reader comments

124 with 74 posters participating

Share this story

Charter can charge Netflix and other online video streaming

services for network interconnection despite a merger condition prohibiting the practice, a federal appeals court ruled today.

The ruling by the US Court of Appeals for the District of Columbia Circuit overturns two merger conditions that the Obama administration imposed on Charter when it bought Time Warner Cable and Bright House Networks in 2016. The FCC under Chairman Ajit Pai did not defend the merits of the merger conditions in court, paving the way for today's ruling. The case was decided in a 2-1 vote by a panel of three DC Circuit judges.

The lawsuit against the FCC seeking to overturn Charter merger conditions was filed by the Competitive Enterprise Institute (CEI), a free-market think tank, and four Charter users who claim they were harmed by the conditions. The FCC unsuccessfully challenged the suing parties' standing to sue, and it did not mount a legal defense of the conditions themselves.

Though Charter did not file this lawsuit, the ISP separately asked the FCC to let the network-interconnection condition and a condition prohibiting data caps expire on May 18, 2021, two years earlier than scheduled. Today's court's ruling seems to render Charter's petition moot as far as the network-interconnection condition goes, but the court ruling did not overturn the data-cap prohibition.

Charter is the second biggest cable company in the US after Comcast and offers service in 41 states under the Spectrum brand name.

ISPs extract payments from online video

The Obama-era FCC required Charter to provide free

interconnection to large online providers until 2023. The condition was intended to prevent business disputes that have a history of harming consumer-broadband performance when companies refuse to pay fees demanded by ISPs.

“Many interconnection agreements are made between broadband Internet providers and ‘edge providers’ such as Netflix—i.e., those who provide content to consumers through the Internet,” today’s ruling noted. “Since broadband providers allow edge providers to reach their subscribers, the broadband providers often can extract payments from edge providers. The disputed condition prohibits New Charter [the post-merger entity] from doing so.”

The CEI lawsuit argued that requiring Charter to forgo revenue from interconnection agreements caused Charter to increase broadband prices after the merger. Of course, Charter could have simply pocketed extra interconnection revenue and still raised Internet prices, as it faces little competition from other high-speed broadband providers in its cable territory. But DC Circuit judges agreed with the plaintiffs’ argument:

> *To begin, the condition plainly caused New Charter to forgo revenue from edge providers. Before the merger, Time Warner, the largest broadband provider among the merging companies, raised substantial revenue from paid interconnection agreements. So did Bright House. But the merger condition prohibits New Charter from using those same revenue sources.*
>
> *It is also clear that the consumers’ bills increased shortly after the merger. Before the merger, France and Haywood [two of the lawsuit filers] subscribed to Bright House’s broadband service, and Frank subscribed to Time Warner’s. Shortly after, New Charter raised their monthly bills: France’s bill increased about 20 percent, from $84 to $101, Haywood’s about 40 percent, from $51 to $71; and Frank’s about 5 percent, from $75.99 to $79.99.*

“Small financial injury” enough to prove standing

The case turned largely on the question of whether the consumers who sued had standing to challenge the conditions. Even if other factors besides interconnection contributed to the price increases, “the subscribers need not show that prohibiting paid interconnection agreements caused the entirety of the price increases, or even that it caused price increases of some specific amount,” judges wrote. “For standing purposes, even a small financial injury is enough, and the consumers have shown a substantial likelihood that their bills are higher because of the prohibition on paid interconnection agreements.”

The lawsuit targeted four merger conditions, and judges ruled that the plaintiffs had standing to challenge two of them: the interconnection-payment ban and a condition requiring Charter to offer a discount Internet service to people with low incomes. The litigants have standing to challenge the discount-service condition based on the argument that a low-income service causes higher prices for other consumers, the judges found.

With the consumers’ having standing to challenge those two conditions, the FCC’s refusal to defend the conditions on their merits made the judges’ decision easier. Judges wrote that they “need not resolve” all the thorny questions of the case because “there is a simpler ground of decision. The lawfulness of the interconnection and discounted-services conditions are properly before us, yet the FCC declined to defend them on the merits. The agency’s only explanation for doing so was its view that we cannot reach the merits. Having lost on that question, the FCC has no further line of defense.” The two conditions are “vacate[d] given the FCC’s refusal to defend on the merits,” the judges wrote.

The low-income condition required Charter to offer 30Mbps broadband service for no more than $14.99 in service fees and no more than $5 in router rental fees each month, and to enroll at least 525,000 qualifying low-income households by May 2020. Charter complied with the condition with its Spectrum Internet Assist program, which is similar to a low-income program offered by Time Warner Cable before the merger. Under the merger condition, Charter was allowed to raise the base price to $17.99 a month last year. Charter hasn't announced any plans to stop offering the low-income service.

The judges rejected the lawsuit's challenge to the data-cap condition, writing that "there is scant evidence that New Charter would offer usage-based pricing if allowed to do so." The judges also rejected the challenge to a requirement that Charter extend its network to 2 million additional homes and businesses, saying that "New Charter already has built much of the required infrastructure, and its sunk costs in doing so cannot be recovered." The litigants "offer no reason to think that New Charter will abandon the project if now allowed to," and "no reason to think that if New Charter were to abandon the project at this late date, thus ensuring a wasted investment, the decision to do so would somehow lower the prices for its broadband customers," the judges wrote.

"Prices go up because of mergers"

Charter told the FCC in a filing that it doesn't "currently" plan to impose data caps or charge video providers for interconnection, but the company wants the prohibitions lifted because they "put Charter at a competitive disadvantage" and "forc[e] Charter to run its network based on arbitrary merger conditions instead of market conditions." Charter's filing also claimed that broadband plans with data caps are "often popular" with consumers.

We contacted Charter about the court decision today and will

update this article if we get a response.

Matt Wood, VP of policy at consumer-advocacy group Free Press, said in response to the court decision that “prices go up because of mergers, not the tame conditions imposed on them. That’s the whole point of taking out competitors and concentrating power.”

Wood pointed to a Free Press filing to the FCC that he said shows “Charter was delivering better value and getting better financial results for itself than any other big wired ISP. So the notion that either Charter or its customers have suffered from the conditions is a joke, as is any claim by the litigants that unconditioned mergers and monopolies are somehow better for people.”

Disclosure: The Advance/Newhouse Partnership, which owns 13 percent of Charter, is part of Advance Publications. Advance Publications owns Condé Nast, which owns Ars Technica.

https://arstechnica.com/?p=1699205

Trump admin. finally kills off Obama-era rule limiting methane emissions

Enlarge / A natural gas flare from an offshore oil drilling rig in Cook Inlet, Alaska.

reader comments

213 with 98 posters participating

Share this story

The Environmental Protection Agency this week finalized a rule that kills off Obama-era limitations on how much methane, a potent greenhouse gas, oil and natural gas producers are allowed to emit into the atmosphere—even though industry leaders didn't want the changes.

The changes to the rules, known as the New Source Performance Standards (NSPS), remove some segments of the industry from being covered under the existing standards at all, and these changes also lift the methane caps on other segments, the EPA announced on Thursday.

The oil and gas industry basically splits into three big buckets of activity: upstream, meaning the actual drilling for oil or gas; midstream, which is the world of storage and pipelines; and downstream, that last mile where products are refined and sold. The current changes apply to the downstream and midstream segments, as the EPA broke down in a graphic (PDF).

The midstream segment, including storage tanks, compressors, and pneumatic controllers, are no longer regulated under the NSPS at all. Drillers in that upstream segment are still subject to regulation, but that regulation now all but eliminates requirements for businesses to monitor, minimize, and repair methane leaks.

The changes will "reduce regulatory burdens for oil and natural gas entities while protecting human health and the environment," the EPA said in a press release.

What next?

Methane is an incredibly potent greenhouse gas, roughly 30 times more effective at trapping heat than carbon dioxide. The EPA's own analysis (PDF) estimates roughly 400,000 additional short tons of methane will be released into the atmosphere by 2030 under the new standards as compared to the 2016 rule.

Even that number, however, may not be a high enough estimate. Repeated studies have found that the EPA drastically underestimates methane emission from oil and gas production.

"The literature has coalesced—80 percent of papers show that methane from oil and gas leaks is two to three times higher than the EPA's estimates," Robert Howarth, an expert at Cornell University, told The New York Times. "It's crazy to roll back this rule… Twenty-five percent of the human-caused warming over the past 20 years is due to methane. Methane is going up. We need it to go down."

Meanwhile, the rule change, according to the EPA, will provide roughly $83 million in savings and benefits per year to the extraction industry. That's equivalent to about 0.002 percent of the industry's $3.3 trillion in global revenues in 2019—at most, corporate pocket change.

The large players in the industry don't want that pocket change back, either. Representatives for Shell, BP, and Exxon Mobil all told NPR that they would prefer the regulation had been left alone. "The negative impacts of leaks and fugitive emissions have been widely acknowledged for years, so it's frustrating and disappointing to see the administration go in a different direction," Gretchen Watkins, president of Shell's US business, said.

Environmental groups, such as the Environmental Defense Fund, are already planning to sue over the reversal, and they'll likely have company from several states.

“It’s not only negligent, it’s unlawful,” California Attorney General Xavier Becerra said in a written statement. “We won’t sit silently while the EPA allows this super pollutant to rapidly warm our atmosphere.”

https://arstechnica.com/?p=1699029

Ripped chemical bags added to risk of Beirut blast

Enlarge / A view of the Port of Beirut on August 13 after a fire at a warehouse with explosives led to massive blasts on August 4.
Aysu Bicer/Anadolu Agency via Getty Images

reader comments

83 with 61 posters participating

Share this story

Lebanese officials knew that more than half the bags of a 2,750-ton stockpile of ammonium nitrate that caused a deadly explosion in Beirut were damaged six years ago but took no action to dispose of the chemical.

A 2014 inspection report by Beirut port authorities, seen by the Financial Times, labels the chemical as “explosives” and said that 1,950 of the 2,750 one-tonne bags filled with the chemical were “torn.” Photos of the stockpile taken the following year, also seen by the FT, show the huge sacks

appearing to be stacked haphazardly on top of each other and ammonium nitrate spilling from large rips in the industrial bags.

The evidence will increase concerns that negligence and poor management were the root cause of the blast at the port, which killed more than 170 people and devastated the capital. Prime Minister Hassan Diab blamed “political corruption” for the tragedy as he resigned on Monday.

The ammonium nitrate, which can be used in fertilizers and as an explosive, was stored at Beirut port, on the northern tip of the capital, for six years after the load was impounded by Lebanese authorities.

Andrea Sella, professor of inorganic chemistry at UCL, the London university, said that when ammonium nitrate, which is manufactured as small white balls known as prills, is stored in bulk for long periods, it absorbs moisture, gradually crystallizes, expands and becomes “compacted like a large rock.”

This makes it a “loaded bomb” without a detonator. An initial fire at the port, which was captured by videos posted on social media, is likely to have provided the trigger, he said.

“The bags could have been damaged when they were offloaded, but chances are they were damaged because the ammonium nitrate crystallized and expanded and the bags were likely to be put into contact with each other, which would create a continuous, solid mass,” Sella said. “It makes it more dangerous and makes it easier for the explosion to travel through the material. It makes it a much more intense explosion—it all goes up in one go.”

He added it was “a high priority” to dispose of ammonium nitrate if it was damaged.

Enlarge / Women walk past a damaged car on August 13, a week-plus after the Port of Beirut explosions. Getty's suggested caption describes the streets of Beirut as "just like war zones with the destroyed buildings, shattered roads, smelly garbages scattered almost everywhere."
Aysu Bicer/Anadolu Agency via Getty Images

Lebanese authorities, who are conducting an investigation into the blast, have yet to give an explanation as to why it was stored at the port, close to the heart of Beirut, for so long.

Adib Ibrahim, a chemical engineer at Geoflint, a Lebanese engineering geo-environmental consultancy, said that after six months the chemical "should have been classified as hazardous waste" and shipped to another country that has the capacity to dispose of toxic waste.

If that was not possible, the ammonium nitrate should have been "deactivated/decomposed" by heating it to more than 169°C, before being "sealed and sent to a designated landfill," Mr.Ibrahim said.

The ammonium nitrate was offloaded at Beirut's port in 2014

after a ship that had set sail from Georgia and was bound for Mozambique ran into trouble in the Mediterranean Sea. The Rhosus and the crew docked in Beirut, where they got caught up in months of legal battles over debts and unpaid fees related to the vessel.

Fábrica de Explosivos de Moçambique, which specialize in explosives for commercial use, said it had ordered the chemical through Savaro Ltd, which appears to be a UK-registered company that has offices in Cyprus. FEM said it would only have paid for the cargo on delivery.

“This was a standard order, of a material that we use in our commercial activity, always fulfilling all legal requirements and the best international practices in a scrupulous way,” the Maputo-based company said.

Ammonium nitrate is produced in different grades with the higher nitrogen content used for explosives, the lower purity for fertilizers. The stock at the port was almost 35-percent nitrogen, a customs chief told the Lebanese army in late 2015, a leaked official letter shows.

Sella said that level of nitrogen corresponded to “explosives grade stuff.”

“It needed to be treated with significant respect,” he said.

Enlarge / A man tries to fix an electricity cable on the damaged roof of an apartment block facing the Beirut port on August 13, 2020.
Chris McGrath/Getty Images

It was not immediately possible to contact Savaro, which appears to have no website. Its last registered office in the UK is on a short residential street in east London. The building displayed no company signs, a locked metal security gate covered the front door, and nobody answered when the FT visited the address.

Lebanon's "urgent matters court," which typically deals with minor civil and commercial cases, had ruled in mid-2014 that the ammonium nitrate should be offloaded from the foundering vessel and stored at Beirut port, out of concern that its "dangerous" cargo might contaminate the sea and cause environmental damage, according to documents seen by the FT.

The court advised that the public works and transport ministry was responsible for storing the goods in a "suitable place" and said it did not have jurisdiction to sell the ship or its contents. All ministers of public works since 2013 are set to

be questioned in the blast investigation, said a government spokesperson.

In January 2015, Joseph Kareh, a Lebanese lawyer acting on behalf of Savaro, wrote to the urgent matters court asking it to investigate the state of the ammonium nitrate bags. The letter, seen by the FT, said the ammonium nitrate was incurring storage charges for Savaro.

The court then commissioned a report by a chemical expert, which also mentioned that 1,950 of the bags containing the explosive material were damaged, but did not identify them as dangerous. Mr.Kareh said he could not comment because of the investigation.

The FT was not immediately able to find records of further legal action by Savaro to retrieve the cargo after 2015. UK company records show that since incorporating in 2006, Savaro has frequently filed accounts as a “dormant” firm.

Savaro’s manager, Greta Bieline, a Lithuanian national, is the director of eight Cyprus-based companies registered in the UK, only three of which are still active. It was not immediately possible to contact Ms. Bieline. When contacted by Reuters news agency, she declined to answer questions.

Customs officials, some of whom have been detained for questioning by Lebanese military police investigating the blast, have said that they warned about the deadly explosives stored at the port multiple times.

Normally when goods are left unclaimed in the port for six months, the customs authorities have the right to impound them and after a further three months, sell the goods at auction. But the ammonium nitrate stayed in the port warehouse for six years.

There appeared to be renewed interest by Lebanese authorities in the stockpile earlier this year. In January, the director-

general of state security requested an investigation into the ammonium nitrate, according to a government spokesman. The request led to an exchange of correspondence between judges and government officials, but the prime minister's office said it was only told about the neglected chemicals two weeks before the explosion. Lebanon's president, Michel Aoun, has said he was also informed about the stockpile this year.

A report compiled by the state security agency, which was sent to the prime minister's office weeks before the blast, said the warehouse where the ammonium nitrate was held was "intended for preserving dangerous materials." It criticized Beirut port for "negligence" in securing the warehouse, risking the "theft of dangerous materials."

The port authorities did not respond to a request for comment.

Additional reporting by Asmaa al-Omar in Istanbul, Joseph Cotterill in Johannesburg, Michael Pooler in London.

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

https://arstechnica.com/?p=1699096

Appeals court ruling for Qualcomm "a victory of theory over facts"

Aurich Lawson / Getty Images

reader comments

69 with 46 posters participating

Share this story

A federal appeals court has tossed out a lower court ruling that Qualcomm abused its dominance of the modem chip market to force customers to pay inflated royalties for its patent portfolio. The appeals court forcefully rejected Judge Lucy Koh's 2019 analysis of Qualcomm's business practices and held that Qualcomm's behavior was merely "hypercompetitive," not anticompetitive.

The two rulings could not have been more different. In last year's 233-page ruling, Judge Koh explained Qualcomm's business practices in so much detail that it took us more than 3,500 words just to summarize her findings. This week's ruling by the Ninth Circuit Appeals Court was shorter—56 pages—and more theoretical.

The appeals court acknowledged that "from 2006 to 2016, Qualcomm possessed monopoly power in the CDMA modem chip market, including over 90% of market share." However, the court found that the Federal Trade Commission—which brought the lawsuit against Qualcomm—had failed to prove that Qualcomm had abused that power. The court reasoned that Qualcomm's licensing practices were simply designed to maximize the company's revenue—and that in itself isn't illegal.

"The plaintiff must show that diminished consumer choices and increased prices are the result of a less competitive market due to either artificial restraints or predatory and exclusionary conduct," the appeals court ruled.

Judge Koh thought the FTC *had* demonstrated predatory and exclusionary conduct. She described how Qualcomm threatened to abruptly cut off the modem chip supply of smartphone makers who challenged Qualcomm's high patent rates. She found

Qualcomm structured deals with Apple, Samsung, LG, and other smartphone vendors to discourage them from doing business with other chipmakers. She cited internal documents in which Qualcomm executives acknowledged the anticompetitive impact of these policies.

But three judges from the Ninth Circuit Appeals Court ignored much of this evidence and waved the rest away.

“I would describe it as a victory of theory over facts,” said Tim Wu, a legal scholar at Columbia University. Wu told Ars that the Ninth Circuit showed “an indifference to the actual effects” of Qualcomm’s conduct.

How Qualcomm boxed out competitors

Qualcomm refused to sell chips to anyone who hadn’t already agreed to license Qualcomm’s patent portfolio—a policy known as “no license, no chips.” The loss of access to Qualcomm’s modem chips was a powerful threat because Qualcomm held a near monopoly on some categories of cellular modems.

In a 2014 internal email, for example, a Qualcomm executive wrote that Qualcomm’s stranglehold over the CDMA market gave the company a lot of leverage in negotiations with Apple. At the time, the CDMA standard was used by Verizon and Sprint in the United States and some other carriers overseas. Without Qualcomm’s chips, Apple might not have been able to sell phones for those networks.

“We are the only supplier today that can give them a global launch,” the Qualcomm executive wrote. “Without us they would lose big parts of North America, Japan and China. That would really hurt them.”

That leverage enabled Qualcomm to charge what the FTC—and Judge Koh—considered to be inflated patent royalty rates. But those high rates depended on maintaining Qualcomm’s dominance.

One way Qualcomm prevented rivals from gaining traction was refusing to license its patents to other chipmakers. Ordinarily, a chip vendor is expected to license necessary patents on behalf of its customers. But Qualcomm rejected licensing requests from other chipmakers, insisting instead that smartphone vendors obtain a license directly from Qualcomm.

As a result, Qualcomm was able to charge a fee to every smartphone maker whether or not they purchased Qualcomm's chips. Qualcomm demanded royalties based on the price of the entire smartphone, not just on the value of the chips that were covered by Qualcomm's patents. In effect, Judge Koh ruled, Qualcomm imposed a tax on the sale of non-Qualcomm chips.

Patent shenanigans

Even worse, Judge Koh pointed out that Qualcomm had previously agreed to license many of its patents—those necessary to implement wireless standards—on fair, reasonable, and non-discriminatory (FRAND) terms. In Koh's view, Qualcomm broke that commitment when it refused to license its patents to other chipmakers. Qualcomm also insisted that smartphone makers license its non-FRAND patents along with the FRAND patents, another potential violation of FRAND rules.

Qualcomm offered other chipmakers a promise not to sue them for patent infringement without charge. In this week's ruling, the Ninth Circuit characterized this as a harmless "no license, no problem" policy. But Mark Patterson, an antitrust scholar at Fordham University, told Ars that this wasn't quite accurate.

In exchange for a promise not to sue, Qualcomm demanded that rivals provide access to their sales data, which is normally considered a sensitive trade secret. This data helped to guide Qualcomm's efforts to prevent other chip companies from

gaining traction in the market.

And Qualcomm knew exactly what it was doing, as this comically candid 2009 slide from an internal presentation illustrates:

Qualcomm’s strategy was to make sure that MediaTek—a rival supplier of modem chips—could only do business with companies that had a Qualcomm patent license (referred to as “WCDMA SULA”), thereby limiting MediaTek to around 50 customers. Having fewer customers made it harder for MediaTek to achieve the scale required to sell 3G chips profitably. Meanwhile, Qualcomm aimed to “destroy” MediaTek’s profits in the older 2G market, depriving MediaTek of cash it could invest in 3G chips.

This slide went unmentioned by the Ninth Circuit as it dismissed claims that Qualcomm had harmed competition.

https://arstechnica.com/?p=1698262

NSA and FBI warn that new Linux malware threatens

national security

reader comments

83 with 55 posters participating, including story author

Share this story

The FBI and NSA have issued a joint report warning that Russian state hackers are using a previously unknown piece of Linux malware to stealthily infiltrate sensitive networks, steal confidential information, and execute malicious commands.

In a report that’s unusual for the depth of technical detail from a government agency, officials said the Drovorub malware is a full-featured tool kit that has gone undetected until recently. The malware connects to command and control servers operated by a hacking group that works for the GRU, Russia’s military intelligence agency that has been tied to more than a decade of brazen and advanced campaigns, many of which have inflicted serious damage to national security.

“Information in this Cybersecurity Advisory is being disclosed publicly to assist National Security System owners and the public to counter the capabilities of the GRU, an organization which continues to threaten the United States and U.S. allies as part of its rogue behavior, including their interference in the 2016 US Presidential Election as described in the 2017 Intelligence Community *Assessment, Assessing Russian Activities and Intentions in Recent US Elections* (Office of the Director of National Intelligence, 2017),” officials from the agencies wrote.

Stealthy, powerful, and full featured

The Drovorub toolset includes four main components: a client that infects Linux devices; a kernel module that uses rootkit tactics to gain persistence and hide its presence from operating systems and security defenses; a server that runs on attacker-operated infrastructure to control infected machines and receive stolen data; and an agent that uses compromised servers or attacker-control machines to act as an intermediary between infected machines and servers.

A rootkit is a type of malware that burrows deep inside an operating system kernel in a way that prevents the interface from being able to register the malicious files or the processes they spawn. It uses a variety of other techniques as well to make infections invisible to normal forms of antivirus. Drovorub also goes to great lengths to camouflage traffic passing into and out of an infected network.

The malware runs with unfettered root privileges, giving operators complete control of a system. It comes with a full menu of capabilities, making a malware equivalent of a Swiss Army knife.

Security driver slayer

Government officials said Drovorub gets its name from strings unintentionally left behind in the code. “Drovo” roughly translates to “wood” or “firewood,” while “rub” translates to “fell” or “chop.” Put together, the government said, Drovorub means “woodcutter” or to “split wood.” Dmitri Alperovitch, a security researcher who has spent most of his career investigating Russian hacking campaigns—including the one that targeted the DNC in 2016—offered a different interpretation.

“Re: malware name ‘Drovorub,’ which as @NSACyber points out

translates directly as ‘woodcutter,’” Alperovitch, a co-founder and former CTO of security firm CrowdStrike, wrote on Twitter. “However, more importantly, ‘Drova’ is slang in Russian for ‘drivers,’ as in kernel drivers. So the name likely was chosen to mean “(security) driver slayer.”

> *Re: malware name “Drovorub”, which as @NSACyber points out translates directly as “woodcutter”*
>
> *However, more importantly, “Drova” is slang in Russian for “drivers”, as in kernel drivers. So the name likely was chosen to mean “(security) driver slayer” https://t.co/yToULwp3xw*
>
> *— Dmitri Alperovitch (@DAlperovitch) August 13, 2020*

Serving Russia’s national interests for more than a decade

Drovorub adds to an already abundant cache of previously known tools and tactics used by APT 28, the Russian military hacking group that other researchers call Fancy Bear, Strontium, Pawn Storm, Sofacy, Sednit, and Tsar Team. The group’s hacks serve Russian government interests and target countries and organizations the Kremlin considers adversaries.

In August, Microsoft reported that the group had been hacking printers, video decoders, and other so-called Internet-of-things devices and using them as a beachhead to penetrate the computer networks they were connected to. In 2018, researchers from Cisco’s Talos group uncovered APT 28’s infection of more than 500,000 consumer-grade routers in 54 countries that could then be used for a range of nefarious purposes.

Other campaigns tied to APT 28 include:

Thursday’s advisory didn’t identify the organizations Drovorub

is targeting or provide even broad descriptions of the targets or geographies where they're located. It also didn't say how long the malware has been in the wild, how many known infections there have been to date, or how the hackers are infecting servers. APT 28 often relies on malicious spam or phishing attacks that either infect computers or steal passwords. The group also exploits vulnerabilities on devices that haven't been patched.

Required reading

Agency officials said that a key defense against Drovorub is to ensure that all security updates are installed. The advisory also urged that, at a minimum, servers run Linux kernel version 3.7 or later so that organizations can use improved code-signing protections, which use cryptographic certificates to ensure that an app, driver, or module comes from a known and trusted source and hasn't been tampered with by anyone else.

"Additionally, system owners are advised to configure systems to load only modules with a valid digital signature making it more difficult for an actor to introduce a malicious kernel module into the system," the advisory stated.

Also included are rules that network administrators can plug in to the Yara and Snort intrusion detection systems to catch and halt network traffic passing to or from control servers or to flag obfuscated Drovorub files or processes already running on a server.

The 45-page document provides a level of technical detail and informed analysis that's on par with some of the best research from private companies. The advisory is also the first to disclose the existence of this new and advanced malware. Those are things that are rarely available in government advisories. The report should be required reading for anyone managing a network.

https://arstechnica.com/?p=1698939

Epic files suit against Apple after Fortnite pulled from iOS App Store [Updated]

Enlarge / *Fortnite* seen in the App Store on an iPhone on May 10, 2018.

reader comments

697 with 253 posters participating

Share this story

Update 7:05pm EST: Google has now followed Apple's lead, removing *Fortnite* from the Google Play store (that link goes to the former Play store page for the game). You can still download *Fortnite* on Android directly from Epic.

"The open Android ecosystem lets developers distribute apps through multiple app stores," Google said in a statement. "For game developers who choose to use the Play Store, we have consistent policies that are fair to developers and keep the store safe for users. While *Fortnite* remains available on Android, we can no longer make it available on Play because it violates our policies. However, we welcome the opportunity to continue our discussions with Epic and bring *Fortnite* back to Google Play."

Two years ago, Epic voluntarily pulled *Fortnite* from the Google Play store in an attempt to get around the platform's 30 percent revenue cut. Though Epic drew millions of direct downloads without a Google Play listing, Epic reversed course and brought the game back to Google Play this April.

"Google puts software downloadable outside of Google Play at a disadvantage," Epic said in April, "through technical and business measures such as scary, repetitive security pop-ups for downloaded and updated software, restrictive manufacturer and carrier agreements and dealings, Google public relations characterizing third-party software sources as malware, and new efforts such as Google Play Protect to outright block software obtained outside the Google Play store."

Update 4:05pm EST: In a video message premiering in *Fortnite*'s own Party Royale mode, Epic wrote that it has "defied the App Store Monopoly. In retaliation, Apple is blocking *Fortnite* from a billion devices. Join the fight to stop 2020 from becoming '1984.'"

The video directly parodies Apple's famous 1984 Macintosh advertisement, down to an Apple executive stand-in saying that users have "given us their songs, their labor, their dreams. In exchange we have taken our tribute, our profits, our control. This power is ours and ours alone. We shall prevail."

The movie ends with the hashtag #FreeFortnite.

[embedded content]
Update 3:45pm ET: Less than an hour after *Fortnite* was removed from the iOS App Store, Epic announced it has filed a complaint for injunctive relief with a Northern District of California federal court.

The 61-page document makes reference to Apple's famous *1984* Macintosh ad, arguing that today, "Apple has become what it once railed against: the behemoth seeking to control markets, block competition, and stifle innovation. Apple is bigger,

more powerful, more entrenched, and more pernicious than the monopolists of yesteryear. At a market cap of nearly $2 trillion, Apple's size and reach far exceeds that of any technology monopolist in history."

Epic is seeking an injunction against Apple's "anti-competitive conduct" and a decision finding that Apple's developer terms regarding App Store approval and in-app purchases are "unenforceable."

Update 3:04pm ET: Apple removed *Fortnite* from appearing on the iOS App Store by 2:50pm. As of 3pm, the game still remains available on Google's Play Store.

Apple in a statement described Epic's move as an "unfortunate step." The statement continued:

> *Epic enabled a feature in its app which was not reviewed or approved by Apple, and they did so with the express intent of violating the App Store guidelines regarding in-app payments that apply to every developer who sells digital goods or services…*
>
> *Epic agreed to the App Store terms and guidelines freely and we're glad they've built such a successful business on the App Store. The fact that their business interests now lead them to push for a special arrangement does not change the fact that these guidelines create a level playing field for all developers and make the store safe for all users. We will make every effort to work with Epic to resolve these violations so they can return Fortnite to the App Store.*

Original Story:

In a move seemingly calculated to be both an enticement to players and a middle finger aimed directly at Apple and Google, game developer Epic today began offering a discount for *Fortnite* players who use Epic's own direct payment system

for in-game purchases.

The “Fortnite Mega Drop” is a permanent 20-percent discount on purchases across all platforms, Epic announced today. Players on traditional consoles (Playstation 4, Xbox One, and Nintendo Switch) and on PC or Mac computers will get the discount automatically. Players on iOS and Android can choose between Apple App Store / Google Play Store at the regular price or, immediately below, the same item through Epic direct payment at a discount. Players who purchased V-Bucks or real-money items since July 14 will also see a retroactive bonus, Epic said.

Epic is not shy about explaining its reasoning. “Currently, there are no savings if players use Apple and Google payment options, where Apple and Google collect an exorbitant 30% fee on all payments,” the company said. “If Apple and Google lower their fees on payments, Epic will pass along the savings to players.”

Enlarge / A sample of how *Fortnite* mobile transactions will now look, according to Epic.

Fortnite initially launched on Android outside of the Google Play Store, explicitly citing Google's 30-percent cut of revenues as a reason why. (It is not possible for apps to launch on iOS outside of Apple's App Store.) In April, however, Epic gave up on side-loading and moved to the Play Store.

"Google puts software downloadable outside of Google Play at a disadvantage," Epic said at the time, adding that Google employs "technical and business measures such as scary, repetitive security pop-ups for downloaded and updated software, restrictive manufacturer and carrier agreements and

dealings, Google public relations characterizing third-party software sources as malware, and new efforts such as Google Play Protect to outright block software obtained outside the Google Play store."

Tim Sweeney, Epic's founder and CEO, has been expressing dissatisfaction with Apple's cut of in-app purchases for months. "Apple has gone crazy," he wrote in a series of tweets last month. "Truly, Apple has no right to take any percent of any company's revenue just because they made the phone people use to access the stuff." He went on:

> *If Apple had the way, they'd block the web and make arbitrary decisions about what pages you're allowed to visit … and then demand 30% of the revenue from every company that does business on the web. The tying of the operating system to a monopoly software distribution channel and monopoly payment processor and monopoly tax doesn't need "policy tweaks," it needs to stop. All of these components must be unbundled to support fair competition among stores, apps and suppliers.*

Join the club

Epic is the latest in a long line of app developers worldwide to reach a breaking point with Apple and Google over mobile distribution.

European Union regulators this summer opened a formal investigation into Apple's pricing strategy following a 2019 complaint from Spotify. "Apple requires that Spotify and other digital services pay a 30% tax on purchases made through Apple's payment system, including upgrading from our Free to our Premium service," Spotify founder and CEO Daniel Ek wrote at the time. "If we pay this tax, it would force us to artificially inflate the price of our Premium membership well above the price of Apple Music. And to keep our price competitive for our customers, that isn't something we can

do.”

Messaging app Telegram also filed a complaint with EU regulators this year about Apple’s App Store. And ProtonMail founder and CEO Andy Yen earlier this month wrote a blistering post that accused Apple of “holding all of us hostage,” adding that its policy is “virtually indistinguishable from a protection racket.”

US regulators are also questioning if Apple’s take is within the boundaries of competition law. Reps. Hank Johnson (D-Ga.) and Lucy McBath (D-Ga.) took Apple CEO Tim Cook to task during a marathon antitrust hearing last month, after a year-long probe into the company’s business found that some major developers, such as Amazon, were able to negotiate preferential treatment.

Google and Apple are also both facing antitrust probes by the Department of Justice relating to their business practices. The details of those probes are not public, but the App Store and Play Store are both widely believed to be among the topics under investigation.

Kyle Orland contributed to this report.

https://arstechnica.com/?p=1698645

Ousted COO sues Pinterest, alleges rampant gender discrimination

Enlarge / A Pinterest logo seen displayed on a smartphone.

reader comments

81 with 57 posters participating

Share this story

The former chief operating officer of Pinterest is suing her ex-employer, claiming that the platform's woman-friendly public face is not matched internally and instead "reflects a pattern of discrimination and exclusion."

Pinterest hired Francoise Brougher as chief operating officer in March 2018, then fired her in April of this year. In a lawsuit (PDF) Tuesday in California, Brougher claims that her dismissal was unrelated to her performance and was instead in retaliation for complaining about sexism.

Brougher learned in 2019, while reviewing filings that Pinterest was required to make as part of its IPO, that she had been deliberately misled about executive compensation. She was therefore being paid less well than other C-suite executives, the suit alleges. After she brought the discrepancy to the attention of Chief Executive Officer Ben Silbermann, she began being squeezed out of executive and board meetings, Brougher alleged, which prevented her from being able to do her job.

"I believe that I was fired for speaking out about the rampant discrimination, hostile work environment, and misogyny that permeates Pinterest," Brougher wrote in a personal essay about the lawsuit." It is time to eliminate the 'boys clubs' that dominate far too many companies and make room for more women leaders and their ideas."

Beyond the C-suite

Brougher is not the first to claim Pinterest fostered a hostile work environment. Two Black women who formerly worked on Pinterest's policy team, Ifeoma Ozoma and Aerica Shimizu Banks, both publicly disclosed in June that they left the company after experiencing and observing rampant discrimination in the office.

"My manager made disparaging comments about my ethnicity in front of my team, and later about another woman colleague's Jewish heritage in relation to those earlier comments. It was wild," Banks wrote in a tweet. She took the complaint to HR, she added, "and this is when the retaliation began."

"I am SO proud of the initiatives I led in my time [with Pinterest]," Ozoma wrote. "I just wish it wasn't sullied by the racism, gaslighting, & disrespect from my manager, skip level, and the company's legal & HR leadership."

In the wake of their allegations going viral, Ozoma, Banks, and several other Pinterest employees spoke with The Washington Post about their experiences with discrimination inside the company:

> *One black female former employee said she was told to stop speaking in meetings and watched her manager use the presentations she created to speak to clients instead. The woman, who was the only black person on her team, said an executive joked that she should act as "the servant" and "serve" her co-workers at a team dinner. "Everyone knew it was wrong, but nobody said anything in that moment," said the ex-employee, who said she was too scared of retaliation to report the incident to HR.*

Beyond Pinterest

Gender-based discrimination is one of Big Tech’s longest-standing problems, and lawsuits are not new.

Former Reddit CEO Ellen Pao made international headlines for her 2012 lawsuit against her former firm, Kleiner Perkins, in which she alleged systematic gender discrimination.

In 2017, a group of former Google employees alleged widespread pay discrimination and sued the firm, echoing allegations the Department of Labor filed against the company. That same year, a group of employees sued Oracle—which was also facing a federal suit—with similar allegations. Tesla, too, was sued for gender discrimination that year.

Businesses large and small have sworn to do better in the years since, but change is, at best, slow to develop. Google’s most recent internal diversity report (PDF) found that less than one-third of the company’s employees globally are women—and only 26.7 percent of company leadership roles are occupied by women. At Facebook, a total of 37 percent of the company’s workforce are women, which drops to 34 percent in leadership roles. At Amazon, 42.7 percent of employees are women—but only 27.5 percent of managers and company leaders are.

The same day Brougher sued Pinterest, a former SoulCycle employee filed suit against the exercise technology firm, claiming the company discriminated against her and other employees when they became pregnant or took maternity leave.

https://arstechnica.com/?p=1698370