FCC lowers some prison phone rates after blaming states for high prices

reader comments

43 with 34 posters participating, including story author

Share this story

The Federal Communications Commission today voted unanimously to lower the prices inmates pay for phone calls from prisons and jails, but the organization reiterated its position that state governments must take action to lower prices on the majority of inmate calls.

Today's action is a proposal to "substantially reduce [the FCC's] interstate rate caps—currently $0.21 per minute for debit and prepaid calls and $0.25 per minute for collect calls—to $0.14 per minute for debit, prepaid, and collect calls from prisons, and $0.16 per minute for debit, prepaid, and collect calls from jails." This is part of a Notice of Proposed Rulemaking, which means the commission will take public comment before finalizing the new caps and could change the plan before making it final.

Since the proposed rate cap limits prices on interstate calls only, it won't affect the approximately 80 percent of prison calls that don't cross state lines. Last month, FCC Chairman Ajit Pai urged state governments to cap intrastate calling prices, saying the FCC lacks authority to do so. Pai said that "33 states allow rates that are at least double the current

federal cap, and 27 states allow excessive ‘first-minute’ charges up to 26 times that of the first minute of an interstate call.”

Prison phone companies Global Tel*Link and Securus Technologies have repeatedly challenged FCC-imposed rate limits in court. But while the Obama-era FCC fought in court to lower intrastate rates, Pai in January 2017 instructed FCC lawyers to drop the commission’s court defense of the FCC cap on intrastate calling rates. The FCC might have lost that case anyway, as previous court rulings went against the commission. But Pai’s decision to drop the court defense helped ensure that the FCC wouldn’t be able to cap intrastate rates.

Today’s FCC announcement said “the commission urges its state partners to take action to address the egregiously high intrastate ICS [inmate calling services] rates across the country.”

FCC limits add-on fees

The FCC did take one other action today that should lower some of the “ancillary” fees prison phone companies apply to both interstate and intrastate calls. Limits approved by the Obama-era FCC say that prison phone companies can’t charge more than $3 for making automated payments by phone or website; $5.95 for making payments with a “live agent;” and $2 for “paper bill fees.” The Obama-era FCC also voted to ban other ancillary service charges.

The FCC vote today ensures that these limits can be applied to intrastate calls in some circumstances. The FCC noted that the June 2017 ruling by the US Court of Appeals for the District of Columbia Circuit “directed the Commission to consider whether these [ancillary] charges can be segregated into interstate and intrastate components for the purpose of excluding the intrastate components from the reach of the FCC’s rules.” The FCC continued:

> *Today's Order finds that, as a practical matter, these charges cannot be segregated between interstate and intrastate calls except in a limited number of cases. As a result, ICS providers are generally subject to the FCC's rules when it comes to ancillary service charges. This means that ICS providers generally cannot charge incarcerated individuals and their families ancillary service charges other than the types allowed by the Commission's rules and providers generally cannot charge ancillary service fees above the Commission's applicable fee caps.*

Prison phone providers won't have to follow the FCC ancillary-fee limits in all cases, though. Take the $3 limit on fees for making automated payments; the FCC noted in a draft of today's order that "automated payments fund prepaid or debit accounts that can be used to pay for inmate calling services," and these prepaid or debit accounts can be used to make both interstate and intrastate calls.

"When automated payments cannot be segregated by jurisdiction, they are subject to our ancillary service charge rules," including the $3 limit, the FCC said. But in cases where an automated payment is made after calls are made, and in which the provider "can confirm that not one call with an outstanding balance was made that crossed state lines," the providers could still tack fees higher than $3 onto those payments.

The FCC also said that an ancillary fee applied to a single intrastate call "is beyond the reach of our regulations," giving providers leeway to impose extra fees on individual calls.

FCC order welcome but long

“overdue”

Despite those limits, the FCC decision was seen as step forward. “By claiming jurisdiction over ancillary fees, the FCC has moved to apply the agency’s uniform rate caps to the fees permitted under the FCC rules instead of allowing differing—and often higher—state charges for these services,” consumer-advocacy group Public Knowledge said today. Public Knowledge also said the FCC should consider even lower caps on interstate rates than the 14¢-per-minute limit tentatively approved today, and the group urged Congress to explicitly allow the FCC to regulate intrastate rates.

FCC Commissioner Jessica Rosenworcel, one of two Democrats on the Republican-majority agency, said at today’s FCC meeting that “today’s order is welcome, even if it is overdue.” She noted that the order came “more than three years after a court sent our work on this issue back to the agency” and that the FCC first received a petition to lower inmate calling rates 17 years ago. The price of a single call from prison “can be as much as many of us pay for unlimited monthly plans,” Rosenworcel said.

“This agency should be embarrassed,” Rosenworcel said. “The fact that it has taken us so long to fix this problem is especially shameful now as we wrestle with a health crisis that has made our prisons less safe and in-person visits no longer viable.”

https://arstechnica.com/?p=1697219

Trump campaign’s false COVID-19 claims taken down by Facebook and Twitter

Aurich Lawson / Getty Images

reader comments

236 with 105 posters participating

Share this story

For the first time, both Facebook and Twitter acted to remove content shared by the campaign to re-elect President Donald Trump from their platforms, citing policies against spreading false claims about COVID-19.

Both the @TeamTrump campaign Twitter account and the official Donald Trump Facebook account shared a video late yesterday in which Trump claimed children are immune from the novel coronavirus. The video was a clip from an interview in which the president spoke by phone with *Fox & Friends* hosts about schools reopening this fall. “My view is that schools should be open,” Trump said. “If you look at children, children are almost—and I would almost say definitely—but almost immune from this disease. So few, they’ve got stronger, hard to believe, I don’t know how you feel about it, but they have much stronger immune systems than we do somehow for this. They don’t have a problem. They just don’t have a problem. They are virtually immune from this problem.”

Children are in fact people and are just as susceptible as the rest of us to breathing in and sneezing out germs. (Possibly

more so, if you ask any parent of a toddler.) Kids do, on average, tend to have much less severe cases of COVID-19 than adults when they catch it, but repeated outbreaks in camps and schools since June have made it abundantly clear that children can both catch and transmit the virus.

Facebook, which has until now taken a hands-off stance with the Trump account when it spreads misinformation and false claims, was first to remove the post. “This video includes false claims that a group of people is immune from COVID-19 which is a violation of our policies around harmful COVID misinformation,” a company rep said in a statement.

Twitter followed suit shortly thereafter, hiding the post and temporarily suspending the Team Trump account until the account deleted the offending post. The post violated the Twitter rules against COVID-19 misinformation, a spokesperson said, adding, “The account owner will be required to remove the tweet before they can tweet again.” The account did indeed take down the post and addressed the matter this morning with a tweet that tagged in Twitter and Facebook and said only, “STOP THE BIAS!”

New call

Twitter has for several months shown an increasing willingness to take action when accounts affiliated with Trump break its rules. In late May, the platform appended a fact check notice to a tweet from Trump that claimed all mail-in voting is inherently fraudulent. (It is not.) Shortly after, another Trump tweet, which was also shared by the official White House account, had a rulebreaker warning tacked onto it when Twitter found it to be in violation of its policy against glorifying violence. And just last week, the site temporarily suspended the account of Donald Trump Jr. for posting false COVID-related claims.

For Facebook, meanwhile, this action is a first. The platform

has to date been infamously reticent to do anything when high-profile accounts post content that would otherwise be against its rules. Politicians are explicitly exempt from both hate speech rules and the fact-checking process, Facebook has repeatedly said, including in advertising.

In recent weeks, however, and amid widespread criticism, Facebook appears to be fractionally softening its stance. Against the background of the nationwide civil rights protests that followed George Floyd's death, company employees and civil rights groups loudly condemned Facebook CEO Mark Zuckerberg's position on Trump's calls to violence.

In mid-June, Facebook took down a Trump advertising campaign that contained imagery used by the Nazi Party after being contacted by several media outlets about the ads. The company's head of security policy was, in the very moment the ads were taken down, testifying to Congress about Facebook's moderation and content policies.

More than 1,000 organizations took part in a month-long Facebook advertising boycott in July. On June 29, just ahead of the boycott start, Zuckerberg said Facebook would change its policy to begin labeling the rule-breaking messages it leaves up under its public-interest exemption, much in the same way Twitter does.

Too wide a net

Twitter's attempt to contain bad information about COVID-19 unfortunately aimed too wide, also taking down several users' attempts to fact-check Trump's claims.

Multiple reporters and news outlets linked to the video in Tweets that editorialized and/or fact-checked the comment and had their accounts temporarily locked until they, too, deleted tweets including the video links.

The Recount, a news site, shared a screenshot of the warning it received from Twitter over its post, which quoted parts of Trump’s statement and added the dry editorial claim, “This is where we’re at.”

Reporter Bobby Lewis, who often live-tweets along with Trump’s Fox appearances, said he had his account locked several times in the past day for critically quoting Trump or sharing the video in which he made his false COVID-related claims.

Aaron Rupar, an editor with Vox, also posted a message that included excerpt’s from Trump’s interview, adding, “Holy shit… just stunningly irresponsible stuff.” Twitter temporarily suspended his account as well, according to a screenshot he posted. “My account was locked for quoting and fact-checking Trump, and I was forced to delete this tweet,” Rupar wrote. “Why am I getting punished for shining a light on the president’s falsehoods?”

“Accounts that tweeted the video may also be required to remove their tweets,” Twitter spokesperson Liz Kelley explained to Ars, “as it’s the video itself that violates our COVID-19 misinformation policy.”

https://arstechnica.com/?p=1697082

Trump admin shrugs off FCC court loss to fight Calif. net neutrality law

Getty Images | Rafe Swan

reader comments

107 with 61 posters participating

Share this story

The Trump administration and broadband industry are resuming their fight against California's net neutrality law, with the US Department of Justice and ISP lobby groups filing new complaints against the state yesterday.

The case is nearly two years old but was put on hold because California in October 2018 agreed to suspend enforcement of its law until after litigation over the Federal Communications Commission's repeal of US net neutrality rules and the FCC's attempt to preempt state net neutrality laws. That lawsuit was decided in October 2019 when the US Court of Appeals for the District of Columbia Circuit upheld the FCC repeal of its own rules but overturned the FCC's attempt to impose a blanket, nationwide preemption of any state net neutrality law.

"At bottom, the Commission lacked the legal authority to categorically abolish all 50 States' statutorily conferred authority to regulate intrastate communications," judges in that case wrote. But that doesn't prevent the Trump administration and ISPs from trying to block state laws on a case-by-case basis.

The appeals window in the FCC case closed last month, allowing the California case to move forward in US District Court for the Eastern District of California. Now that the Trump administration and broadband industry have filed amended complaints, California has until September 16 to file briefs supporting its net neutrality law.

California's net neutrality law prohibits Internet service providers from blocking or throttling lawful traffic and from

requiring fees from websites or online services to deliver or prioritize their traffic to consumers. The state law also bans paid data cap exemptions (so-called "zero-rating") and says that ISPs may not attempt to evade net neutrality protections by slowing down traffic at network interconnection points.

DOJ: States can't regulate interstate traffic

Despite the FCC's preemption order being overturned in court, the DOJ's amended complaint yesterday argued that California's net neutrality law "is preempted by federal law and therefore violates the Supremacy Clause of the United States Constitution."

"California, however, seeks to second-guess the Federal Government's regulatory approach by enacting SB-822 [the state net neutrality law]," the DOJ said. The state law "also violates the division of regulatory authority between states and the Federal Government" in which the FCC has "exclusive responsibility" for regulating interstate communications "while leaving states with responsibility for intrastate communications," the DOJ said. The California law violates that division because "Internet communications are inherently interstate," the DOJ said.

The DOJ also asked for a preliminary injunction that would prevent enforcement of the California law while the case is pending.

The broadband industry's amended complaint was filed by the major lobby groups representing cable, fiber, DSL, and mobile Internet providers. "This case presents a classic example of unconstitutional state regulation… This statute was purposefully intended to countermand and undermine federal law by imposing on broadband—an interstate communications service—the very same regulations that the Federal

Communications Commission expressly repealed in its 2018 Restoring Internet Freedom Order (and by adopting even more restrictive regulations)," the ISP lobby groups wrote.

Though the FCC's nationwide preemption was already thrown out by the DC Circuit appeals court, ISPs said that "the court did so only because it found the FCC lacked authority to expressly preempt all state regulation of intrastate broadband" and that "the court recognized that some state laws could conflict with, and be preempted by" the FCC preemption order. Additionally, the court decision "did not address whether the Communications Act itself preempted state regulation," ISPs wrote.

The DOJ argued that "importantly, the DC Circuit did not decide 'whether the remaining portions of the [FCC repeal] Order have preemptive effect under principles of conflict preemption or any other implied-preemption doctrine,' noting that a conflict analysis depended on having 'the facts of any alleged conflict before us.' The Court left that issue open for another case where—like here—the Commission makes… provision-specific arguments."

FCC abandoned its Title II authority

California will likely point to other portions of the DC Circuit order, which found that the FCC's power to preempt is limited because the commission abandoned its Title II regulatory authority over broadband. "[I]n any area where the Commission lacks the authority to regulate, it equally lacks the power to preempt state law," judges wrote in that case. The FCC's "affirmative" sources of regulatory authority come from Title II, III, and VI of the Communications Act, judges wrote. But Pai's FCC chose to apply Title I to broadband, which contains no such authority.

A spokesperson for California Attorney General Xavier Becerra told Ars, “We are reviewing the complaints and look forward to defending California’s state net neutrality protections.”

FCC Commissioner Jessica Rosenworcel, a Democrat who voted to impose net neutrality rules during the Obama administration and later opposed Chairman Ajit Pai’s repeal, called the DOJ’s lawsuit “shameful.”

“Millions wrote the FCC to say they supported net neutrality,” Rosenworcel wrote on Twitter yesterday. “But the FCC didn’t listen. It rolled back open Internet policies, over my objection. So states set out to right what the FCC got wrong, in their own laws. Today DOJ went to court to stop California’s effort. Shameful.”

https://arstechnica.com/?p=1697135

Insecure satellite Internet is threatening ship and plane safety

reader comments

36 with 30 posters participating, including story author

Share this story

More than a decade has passed since researchers demonstrated

serious privacy and and security holes in satellite-based Internet services. The weaknesses allowed attackers to snoop on and sometimes tamper with data received by millions of users thousands of miles away. You might expect that in 2020—as satellite Internet has grown more popular—providers would have fixed those shortcomings, but you'd be wrong.

In a briefing delivered on Wednesday at the Black Hat security conference online, researcher and Oxford Ph.D. candidate James Pavur presented findings that show that satellite-based Internet is putting millions of people at risk, despite providers adopting new technologies that are supposed to be more advanced.

Over the course of several years, he has used his vantage point in mainland Europe to intercept the signals of 18 satellites beaming Internet data to people, ships, and planes in a 100 million-square-kilometer swath that stretches from the United States, Caribbean, China, and India. What he found is concerning. A small sampling of the things he observed include:

- A Chinese airliner receiving unencrypted navigational information and other avionics data. Equally worrisome, that data came from the same connection passengers used to send email and browse webpages, raising the possibility of hacks from passengers.
- A system administrator logging into a wind turbine in southern France, some 600 kilometers away from Pavur, and in the process exposing a session cookie used for authentication.
- The interception of communications from an Egyptian oil tanker reporting a malfunctioning alternator as the vessel entered a port in Tunisia. Not only did the transmission allow Pavur to know the ship would be out of commission for a month or more, he also obtained the name and passport number of the engineer set to fix the problem.

- A cruise ship broadcasting sensitive information about its Windows-based local area network, including the log-in information stored in the Lightweight Directory Access Protocol database
- Email a lawyer in Spain sent a client about an upcoming case.
- The account reset password for accessing the network of a Greek billionaire's yacht.

Hacking satellite communications at scale

While researchers such as Adam Laurie and Leonardo Nve demonstrated the insecurity of satellite Internet in 2009 and 2010, respectively, Pavur has examined the communications at scale, with the interception of more than 4 terabytes of data from the 18 satellites he tapped. He has also analyzed newer protocols, such as Generic Stream Encapsulation and complex modulations including 32-Ary Amplitude and Phase Shift Keying (APSK). At the same time, he has brought down the interception cost of those new protocols from as much as $50,000 to about $300.

"There are still many satellite Internet services operating today which are vulnerable to their [the previous researchers'] exact attacks and methods—despite these attacks having been public knowledge for more than 15 years at this point," Pavur told me ahead of Wednesday's talk. "We also found that some newer types of satellite broadband had issues with eavesdropping vulnerabilities as well."

The equipment Pavur used consisted of a TBS 6983/6903 PCIe card/DVB-S tuner, which allows people to watch satellite TV feeds from a computer. The second piece was a flat-panel dish, although he said any dish that receives satellite TV will work. The cost for both: about $300.

Using public information showing the location of geostationary satellites used for Internet transmission, Pavur pointed the dish at them and then scanned the k_u band of the radio spectrum until he found a signal hiding in the massive amount of noise. From there, he directed the PCIe card to interpret the signal and record it as a normal TV signal. He would then look through raw binary files for strings such as “http” and those corresponding to standard programming interfaces to identify Internet traffic.

All unencrypted comms are mine

The setup allows Pavur to intercept just about every transmission an ISP sends to a user via satellite, but monitoring signals the other way (from the user to the ISP) is much more limited. As a result, Pavur could reliably see the contents of HTTP sites a user was browsing or of an unencrypted email the user downloaded, but he couldn’t obtain customers’ “GET” requests or the passwords they sent to the mail server.

Even though the customer may be located in the Atlantic off the coast of Africa and is communicating with an ISP in Ireland, the signal it sends is easily intercepted from anywhere within tens of millions of square kilometers, since the high cost of satellites requires providers to beam signals over a wide area.

Enlarge / An attacker from anywhere within tens of millions of square kilometers can hijack the connection between a ship off the coast of Africa and a ground station in Ireland.
Pavur explained:

> *There are a few reasons the other direction is harder to capture. The first is that the beam connecting a satellite to an ISP's ground station is often more narrow and focused (meaning you have to be within a few dozen miles of the ISP's system to pick up radio waves in that direction). In some cases, ISP's will use a different frequency band to transmit these signals for bandwidth and performance reasons—this means an attack might need equipment that is much harder to pick up commercially and affordably. Finally, even if an ISP just uses a normal wide-beam K>$_u$-band signal, they will normally transmit on a different frequency in each direction. This means an attacker would need a second set of antennas (not too difficult) and would also need to combine the two feeds correctly (slightly more difficulty).*

Et tu, Avionics?

In past years, Pavur focused on transmissions sent to everyday users on land and large ships at sea. This year, he turned his

attention to planes. With the onset of the COVID-19 pandemic causing passenger flying to plummet, the researcher had less opportunity than he planned to analyze passenger communications from entertainment systems, in-flight Internet services, and onboard femtocells used to send and receive mobile signals. (He did, however, see a text message providing a passenger with a coronavirus test.)

But it turned out that the decrease in passenger traffic made it easier to focus on traffic sent to crew members in the cockpit. When one of the crew fat fingered a login to what's known as an electronic flight bag, the flightdeck equipment repeatedly got an HTTP 302 Redirect error to the Wi-Fi service login page. The redirect format included the URL of the original request showing the GET parameters of the flight bag API. The parameters described the specific flight number and its coordinates, information that gave Pavur a good feel for what the device was doing aboard the plane.

Enlarge / An electronic flight bag sending sensitive avionics information through HTTP.
James Pavur

The flight-bag data passed through the same network-address-translation router as entertainment and Internet traffic from passengers. In other words, the same physical satellite antenna and modem were delivering Internet traffic to both the flight bag and passengers. This suggests that any network

segregation that may exist was performed by software rather than through physical hardware separation, which is less prone to hacking.

Session hijacking: The attacker always wins

The use of satellite-based Internet to receive the navigational data puts the crew and passengers at risk of an attack Pavur developed that allows an attacker to impersonate the aircraft with which the ground station is communicating. The hack uses TCP session hijacking, a technique in which the attacker sends the ISP the metadata customers use to authenticate themselves.

Because users' traffic is bounced off a satellite 30,000 kilometers above Earth—a route that typically results in signal latency of about 700 milliseconds—and the attacker's data isn't, the attacker will always beat customers in reaching the ISP.

The session hijacking can be used to cause planes or ships to report incorrect locations or fuel levels, false readings for heating, ventilation, and air conditioning systems, or transmit other sensitive data that's falsified. It can also be used to create denials of service that prevent the vessel from receiving data that's crucial to safe operations.

Enlarge / Capabilities and limitations of TCP session hijacking of satellite Internet.
James Pavur
Pavur explained the hijacking methodology this way:

> *We can convert the bytes from the recording in real-time at the IP-packet layer. Essentially, we wait until we record an entire IP packet from the stream (a matter of milliseconds normally) and then immediately write that packet to disk. As an attacker, you do need to know what kind of data you want to extract from the "noise" of people visiting Facebook and so forth. To do that, you can use IP addresses or other traffic signatures to identify just the most relevant traffic to respond to programmatically.*

A problem in search of a solution

The common reaction Pavur gets after he shares his findings is that satellite-based Internet users should simply use a VPN to prevent attackers from reading or tampering with any data sent. Unfortunately, he said, the handshakes required for each endpoint to authenticate itself to the other results in a

slow-down of about 90 percent. The overhead increases the already-large 700 millisecond latency to a wait that renders satellite Internet almost completely unusable.

And while HTTPS and transport-level encryption for email prevent attackers from reading the body of pages and messages, most domain-lookup queries continue to be unencrypted. Attackers can learn plenty by scrutinizing the data. HTTPS certificates allow attackers to fingerprint servers customers connect to.

Enlarge / Left: an unencrypted DNS response shows a satellite Internet user is visiting Dropbox. Right: a breakdown of the most commonly visited domains.
James Pavur

That information allows attackers to identify users who are worthy of more targeted attacks. Out of 100 ships Pavur pseudo-randomly looked at, he was able to deanonymize about 10 and tie them to specific vessels.

Enlarge / Ships Pavur deanonymized.
James Pavur

The interception of unencrypted navigational charts, equipment failures in the open sea, and the use of vulnerability-riddled Windows 2003 servers also puts users at considerable risk. Combined with the use of insecure channels such as FTP, an attacker might be able to tamper with maritime data to hide a sandbar or use the data to plan physical intrusions.

The sheer scale of the problem put the researcher in a quandary. With tens of thousands of users affected, Pavur was unable to privately notify the vast majority of them. He settled on contacting the largest companies who were transmitting particularly sensitive data in the clear. He ultimately chose not to identify any of the affected users or companies because, he said, the crux of the problem is the result of industrywide protocols that are insecure.

“The goal of my research is to bring out these unique dynamics that the physical properties of space create for cybersecurity, and it’s an area that’s been underexplored,” he said. “A lot of people think that satellites are just normal computers that are a little bit further away, but there’s a lot that’s different about satellites. If we highlight those differences, we can better build security to protect the systems.”

https://arstechnica.com/?p=1696924

Zoombomber crashes court hearing on Twitter hack with Pornhub video

reader comments

88 with 69 posters participating, including story author

Share this story

Zoombombers today disrupted a court hearing involving the Florida teen accused of masterminding a takeover of high-profile Twitter accounts, forcing the judge to stop the hearing. “During the hearing, the judge and attorneys were interrupted several times with people shouting racial slurs, playing music, and showing pornographic images,” ABC Action News in Tampa Bay wrote. A Pornhub video forced the judge to temporarily shut down the hearing.

The Zoombombing occurred today when the Thirteenth Judicial Circuit Court of Florida in Tampa held a bail hearing for Graham Clark, who previously pleaded not guilty and is reportedly being held on $725,000 bail. Clark faces 30 felony charges related to the July 15 Twitter attack in which accounts of famous people like Elon Musk, Bill Gates, Jeff Bezos, and Joe Biden were hijacked and used to push cryptocurrency scams. Hackers also accessed direct messages

for 36 high-profile account holders.

Today, Judge Christopher Nash ruled against a request to lower Clark's bail amount. But before that, the judge "shut down the hearing for a short time" when arguments were interrupted by "pornography… foul language and rap music," Fox 13 reporter Gloria Gomez wrote on Twitter.

"I'm removing people as quickly as I can whenever a disruption happens," Nash said after one Zoombomber interrupted a lawyer. A not-safe-for-work portion of the hearing was posted by a Twitter user here. The first 47 seconds are safe to watch and includes Nash's comment about removing Zoombombers, but the rest of the video includes the Pornhub clip that caused Nash to shut down the hearing.

There were still problems after the hearing resumed, the Tampa Bay Times wrote:

> *Hoping a brief pause would filter out the interrupters, Nash reopened the meeting. But users who disguised their names as CNN and BBC News resumed their interruptions.*
>
> *Nash was ultimately able to rule, declining to lower the bail amount. He did, however, remove a requirement that Clark prove the legitimacy of his assets. Lawyers have said he has $3 million in Bitcoin under his control.*

Judge will require password next time

The court obviously failed to take basic steps to prevent the hearing from being intruded upon. We wrote a guide for securing Zoom meetings in April. Our advice includes making sure meetings are password-protected, using Zoom settings to impose limits on screen sharing, and locking meetings once they are underway to prevent unauthorized people from joining

later.

“Predictably, the Zoom hearing for the 17-year-old alleged Twitter hacker in Fla. was bombed multiple times, with the final bombing of a pornhub clip ending the zoom portion of the proceedings,” security reporter Brian Krebs wrote on Twitter. “How the judge in charge of the proceeding didn’t think to enable settings that would prevent people from taking over the screen is beyond me. My guess is he didn’t know he could.”

Nash said that he’ll require a password next time, according to WFLA reporter Ryan Hughes.

Clark would have to pay $72,500, or 10 percent of the bail, to get out of jail before trial, the Tampa Bay Times wrote. Clark was charged with one count of organized fraud, 11 counts of fraudulent use of personal information, one count of accessing a computer or electronic device without authority, and 17 counts of communications fraud.

https://arstechnica.com/?p=1696860

Ex-Googler Levandowski gets 18 months in prison for trade-secret theft

Enlarge / Anthony Levandowski arrives for a court appearance at the Phillip Burton Federal Building and US Courthouse on November 13, 2019 in San Francisco, California.
Getty Images | Justin Sullivan

reader comments

102 with 54 posters participating

Share this story

Ex-Google engineer Anthony Levandowski yesterday was sentenced to 18 months in prison following his March guilty plea for stealing a confidential document related to Google's self-driving technology.

Levandowski's lawyers last week asked a judge in US District Court for the Northern District of California to let him off without any prison time, arguing that a year of home confinement, a fine, restitution, and community service would be sufficient punishment. The federal government asked for a 27-month prison sentence.

While handing down the 18-month sentence, US District Judge William Alsup said that a sentence without imprisonment would give "a green light to every future brilliant engineer to steal trade secrets," according to a Reuters report. Levandowski was originally charged with 33 counts of stealing trade secrets by downloading thousands of documents to his personal laptop in December 2015 shortly before he left Google to work on his startup, Otto, which was acquired by Uber for a reported $680 million in August 2016. In a plea deal, Levandowksi admitted to stealing one document called "Chauffeur TL weekly updates," which tracked the progress of Google's "Project Chauffeur" that later became Waymo. Prosecutors dropped the other charges.

Levandowski won't have to serve the sentence right away, as Alsup ruled that he can go to prison after the coronavirus pandemic subsides, according to Reuters and other news outlets.

Levandowski also must pay $756K to Waymo

Alsup, a 75-year-old judge who has been at the Northern District court since 1999, described the stolen document as a "competitor's game plan" and called Levandowksi's theft the "biggest trade secret crime I have ever seen," according to Reuters. "Billions [of dollars] in the future were at play, and when those kind of financial incentives are there, good people will do terrible things, and that's what happened here," Alsup said. Uber fired Levandowski in May 2017 after he invoked the Fifth Amendment to avoid answering questions in the legal battle with Google.

Levandowski's lawyers argued that home confinement was appropriate because he had suffered two bouts of pneumonia in recent years and was therefore at high risk of getting COVID-19 in prison. After yesterday's sentencing, Levandowski's lawyers said in a statement that "Anthony deeply regrets his past decisions and, while we are saddened that he will have to spend time in prison, Anthony remains committed to his life's mission of building innovative technologies to improve people's lives," according to The New York Times.

Levandowski, who filed for bankruptcy in March, agreed to pay $756,499 in restitution to Waymo, the Google self-driving company that is now a subsidiary of Google owner Alphabet, the Times wrote. He was originally ordered to pay Waymo $179 million but wasn't able to. Levandowski also must pay a fine of $95,000.

Uber and Waymo agreed to a $244 million settlement in 2018. Lior Ron, another ex-Google employee who cofounded Otto with Levandowski, settled with Waymo for $9.7 million. Ron is still an executive at Uber, and Uber reportedly paid the settlement to Waymo on his behalf.

https://arstechnica.com/?p=1696766

Beware of find-my-phone, Wi-Fi, and Bluetooth, NSA tells mobile users

reader comments

67 with 56 posters participating

Share this story

The National Security Agency is recommending that some government workers and people generally concerned about privacy turn off find-my-phone, Wi-Fi, and Bluetooth whenever those services are not needed, as well as limit location data usage by apps.

“Location data can be extremely valuable and must be protected,” an advisory published on Tuesday stated. “It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations.”

NSA officials acknowledged that geolocation functions are enabled by design and are essential to mobile communications. The officials also admit that the recommended safeguards are impractical for most users. Mapping, location tracking of lost

or stolen phones, automatically connecting to Wi-Fi networks, and fitness trackers and apps are just a few of the things that require fine-grained locations to work at all.

The cost of convenience

But these features come at a cost. Adversaries may be able to tap into location data that app developers, advertising services, and other third parties receive from apps and then store in massive databases. Adversaries may also subscribe to services such as those offered by Securus and LocationSmart, two services that The New York Times and KrebsOnSecurity documented, respectively. Both companies either tracked or sold locations of customers collected by the cell towers of major cellular carriers.

Not only did LocationSmart leak this data to anyone who knew a simple trick for exploiting a common class of website bug, but a Vice reporter was able to obtain the real-time location of a phone by paying $300 to a different service. The New York Times also published this sobering feature outlining services that use mobile location data to track the histories of millions of people over extended periods.

The advisory also warns that tracking often happens even when cellular service is turned off, since both Wi-Fi and Bluetooth can also track locations and beam them to third parties connected to the Internet or with a sensor that’s within radio range.

To prevent these types of privacy invasions, the NSA recommends the following:

> - *Disable location services settings on the device.*
> - *Disable radios when they are not actively in use: disable BT and turn off Wi-Fi if these capabilities are not needed. Use Airplane Mode when the device is not in*

use. Ensure BT and Wi-Fi are disabled when Airplane Mode is engaged.

- *Apps should be given as few permissions as possible:*
  - *Set privacy settings to ensure apps are not using or sharing location data.*
  - *Avoid using apps related to location if possible, since these apps inherently expose user location data. If used, location privacy/permission settings for such apps should be set to either not allow location data usage or, at most, allow location data usage only while using the app. Examples of apps that relate to location are maps, compasses, traffic apps, fitness apps, apps for finding local restaurants, and shopping apps.*
- *Disable advertising permissions to the greatest extent possible:*
  - *Set privacy settings to limit ad tracking, noting that these restrictions are at the vendor's discretion.*
  - *Reset the advertising ID for the device on a regular basis. At a minimum, this should be on a weekly basis.*
- *Turn off settings (typically known as FindMy or Find My Device settings) that allow a lost, stolen, or misplaced device to be tracked.*
- *Minimize Web browsing on the device as much as possible, and set browser privacy/permission location settings to not allow location data usage.*
- *Use an anonymizing Virtual Private Network (VPN) to help obscure location.*
- *Minimize the amount of data with location information that is stored in the cloud, if possible.*

If it is critical that location is not revealed for a particular mission, consider the following recommendations:

- *Determine a non-sensitive location where devices with*

wireless capabilities can be secured prior to the start of any activities. Ensure that the mission site cannot be predicted from this location.

- *Leave **all** devices with any wireless capabilities (including personal devices) at this non-sensitive location. Turning off the device may not be sufficient if a device has been compromised.*
- *For mission transportation, use vehicles without built-in wireless communication capabilities, or turn off the capabilities, if possible.*

Mobile phone use means being tracked

Patrick Wardle, a macOS and iOS security expert and a former hacker for the NSA, said the recommendations are a "great start" but that people who follow the recommendations shouldn't consider them anything close to absolute protection.

"As long as your phone is connecting to cell towers, which it has to in order to use the cell network… AFAIK that's going to reveal your location," Wardle, who is a security researcher at the macOS and iOS enterprise management firm Jamf, told me. "It, as always, is a tradeoff between functionality/usability and security, but basically if you use a phone, assume that you can be tracked."

He said that recent versions of iOS make it easy to follow many of the recommendations. The first time users open an app, they get a prompt asking if they want the app to receive location data. If the user says yes, the access can only happen when the app is open. That prevents apps from collecting data in the background over extended periods of time. iOS also does a good job of randomizing MAC addresses that, when static, provide a unique identifier for each device.

More recent versions of Android also allow the same location permissions and, when running on specific hardware (which usually come at a premium cost), also randomize MAC addresses.

Both OSes require users to manually turn off ad personalization and reset advertising IDs. In iOS, people can do this in Settings > Privacy > Advertising. The slider for Limit Ad Tracking should be turned on. Just below the slider is the Reset Advertising Identifier. Press it and choose Reset Identifier. While in the Privacy section, users should review which apps have access to location data. Make sure as few apps as possible have access.

Change some settings

In Android 10, users can limit ad tracking and reset advertising IDs by going to Settings > Privacy and clicking Ads. Both the Reset Advertising ID and Opt Out of Ads personalization are there. To review which apps have access to location data, go to Settings > Apps & notifications > Advanced > Permission Manager > Location. Android allows apps to collect data continuously or only when in use. Allow only apps that truly require location data to have access, and then try to limit that access to only when in use.

Tuesday’s advisory also recommends people limit sharing location information in social media and remote metadata showing sensitive locations before posting pictures. The NSA also warns about location data being leaked by car navigation systems, wearable devices such as fitness devices, and Internet-of-things devices.

The advice is aimed primarily at military personnel and contractors whose location data may compromise operations or put them at personal risk. But the information can be useful to others, as long as they consider their threat model and weigh the acceptable risks versus the benefits of various settings.

https://arstechnica.com/?p=1696452

EU launching deep probe into Google’s planned $2.1 billion Fitbit buy

Enlarge / Logo of Google is displayed on a smartphone by logo of Fitbit in Brussels, Belgium on August 4, 2020.

reader comments

38 with 22 posters participating

Share this story

Regulators in the European Union are launching a deep investigation into Google’s proposed acquisition of wearables maker Fitbit after expressing concerns that giving Google access to Fitbit’s user data could “distort competition.”

The Commission’s in-depth investigation will examine not only the potential outcomes for the advertising market if the transaction goes through, but it will also look at the effects of the deal on the digital healthcare sector and the potential for Google to lock competitors out of access to Android users.

Data provided by wearable devices “provides key insights about the life and the health situation of the users of these devices,” Margrethe Vestager, the European Commission’s head of competition, said in a written statement. “Our

investigation aims to ensure that control by Google over data collected through wearable devices as a result of the transaction does not distort competition."

Google announced its plan to acquire Fitbit back in November in a transaction valued at $2.1 billion. Any merger or acquisition of that scale draws antitrust attention, both in the US and in the EU, and regulators in every country where the companies operate began their merger review processes.

European merger reviews take place in two phases. In the first phase, competition regulators conduct a preliminary investigation. If they don't identify any real problems with the deal, the companies can go forward with their transaction. If the preliminary investigation does reveal the potential for harms, however, then regulators move to a phase two probe.

Following the phase one investigation, the competition bureau demanded concessions from Google in the acquisition. Sources said at the time that if Google did not meet those terms a protracted investigation would likely follow, and that now seems to be happening.

The transaction is also meeting with deep scrutiny here in the US. Under US law, companies planning a merger over a certain value (currently $94 million) have to submit a notification to both the Federal Trade Commission and Justice Department. Once a company has submitted that filing, regulators have 30 days to take a look at the proposal and determine whether to issue a second request for more information and probe deeper. The DOJ issued such a second request to Google and Fitbit in April, and it's currently reviewing the deal.

Google, meanwhile, is under deep scrutiny for potential antitrust violations basically everywhere. The European Commission is among the many agencies probing its behavior and market dominance, as are the DOJ, the attorneys general of 50 US states and territories, and Congress, which grilled Google

CEO Sundar Pichai, along with the heads of Apple, Amazon, and Facebook, about antitrust matters in a six-hour hearing last week.

https://arstechnica.com/?p=1696388

Twitter faces FTC probe, likely fine over use of phone numbers for ads

reader comments

28 with 24 posters participating

Share this story

Twitter is facing a Federal Trade Commission probe and believes it will likely owe a fine of up to $250 million after being caught using phone numbers intended for two-factor authentication for advertising purposes.

The company received a draft complaint from the FTC on July 28, it disclosed in its regular quarterly filing with the Securities and Exchange commission. The complaint alleges that Twitter is in violation of its 2011 settlement with the FTC over the company's "failure to safeguard personal information."

That agreement included a provision banning Twitter from

“misleading consumers about the extent to which it protects the security, privacy, and confidentiality of nonpublic consumer information, including the measures it takes to prevent unauthorized access to nonpublic information and honor the privacy choices made by consumers.” In October 2019, however, Twitter admitted that phone numbers and email addresses users provided it with for the purpose of securing their accounts were also used “inadvertently” for advertising purposes between 2013 and 2019.

In the filing, Twitter estimates the “range of probable loss” it faces in the probe is between $150 million and $250 million, although it adds that “the matter remains unresolved, and there can be no assurance as to the timing or the terms of any final outcome.”

A common problem

Twitter is not the first social media firm to be investigated for exploiting personal information users provided for security reasons. Last year, the FTC levied a record $5 billion fine on Facebook for repeated privacy violations.

Facebook in 2018 not only started pushing notifications to the phone numbers users provided for 2FA purposes but also was found to be using those numbers for a shadow profile which was used to connect other individuals and advertisers to you.

The bulk of the fine related to Facebook’s actions in the Cambridge Analytica scandal, but the FTC also included in its settlement allegations of exactly the same actions Twitter is now accused of. Facebook also settled with the FTC in 2011 over allegations that it misused users’ data, and its use of personal information provided to it for security purposes was found to violate that agreement.

https://arstechnica.com/?p=1696306

Trump pulls re-nomination of FCC Republican who stood up for First Amendment

Enlarge / FCC Commissioner Michael O’Rielly speaks during an FCC meeting in Washington, DC, on November 16, 2017.

reader comments

215 with 83 posters participating

Share this story

The White House yesterday withdrew its re-nomination of Federal Communications Commission member Michael O’Rielly, a Republican who has not supported President Trump’s attempt to punish social media websites for alleged anti-conservative bias.

Trump had nominated O’Rielly to another five-year FCC term in March, and the nomination was awaiting Senate approval. But the White House unexpectedly withdrew O’Rielly’s nomination, “announc[ing] the action Monday in a notice sent to the Senate, which confirms nominees,” Bloomberg reported. “The notice didn’t provide a reason for the decision.”

O’Rielly’s term technically expired in June 2019, but FCC rules allow him to stay through the end of 2020 even if he isn’t re-confirmed by the Senate. O’Rielly has been on the FCC since 2013.

A White House spokesperson declined comment when contacted by Ars. A spokesperson for O’Rielly also declined comment today but said O’Rielly’s office plans to release a statement on the Trump action.

O’Rielly: Constitution protects “editorial decisions”

O’Rielly, a member of the FCC’s 3-2 Republican majority along with Chairman Ajit Pai and member Brendan Carr said in June that he has “deep reservations” that the FCC has the authority to limit social-media companies’ legal protections in the way Trump demanded in an executive order.

O’Rielly expanded on his views in a speech last week, saying, “The First Amendment protects us from limits on speech imposed by the government—not private actors—and we should all reject demands, in the name of the First Amendment, for private actors to curate or publish speech in a certain way. Like it or not, the First Amendment’s protections apply to corporate entities, especially when they engage in editorial decision making.”

Although O’Rielly clarified that his “critique is not in any way directed toward President Trump or those in the White House,” his statement seems to reject the position taken by Trump. His speech came two days after the Trump administration formally petitioned the FCC to reinterpret Section 230 of the Communications Decency Act in a way that would limit social media platforms’ legal protections for hosting third-party content when the platforms take down content they consider objectionable.

While O’Rielly said Trump has a right “to call for the review of any federal statute’s application,” the commissioner also said those reviews are “subject to applicable statutory and constitutional guardrails.” O’Rielly’s comments “drew

attention of some White House and industry officials," Reuters wrote in a story about Trump pulling the re-nomination.

By contrast, Commissioner Carr has explicitly and repeatedly supported Trump's social media crackdown and criticized Twitter for adding a fact check to Trump's claims that mail-in ballots will be "substantially fraudulent." Carr said that "Twitter made the decision to take on the president of the United States in a partisan, political debate and it did so in a really disingenuous way" and is "punishing speakers based on whether it approves or disapproves of their politics."

Pai yesterday called for a "vigorous debate" on Trump's executive order as the FCC issued a public notice seeking comments on the Trump administration petition. Pai hasn't publicly supported or criticized Trump's petition and hasn't committed to taking any action beyond issuing the call for public comments.

Senator criticized O'Rielly on Ligado approval

O'Rielly's re-nomination was approved by the Senate Commerce Committee on July 22 and is awaiting a vote of the full Senate, but it was facing trouble even before Trump withdrew it. Sen. Jim Inhofe (R-Okla.) last week placed a hold on the nomination until O'Rielly commits to voting to overturn the FCC's unanimous approval of Ligado's plan for a 5G cellular network. Inhofe backed US military claims that the Ligado plan will interfere with GPS, but the FCC said that a 23MHz guard band, power limits, and other FCC-imposed conditions will prevent interference. Pai said that "painstaking technical analysis done by our expert staff" showed that the Ligado network can be deployed safely.

The Ligado decision doesn't appear to be the driving force behind Trump pulling O'Rielly's re-nomination. "According to

sources, the decision to pull back the nomination does not appear to be related to Ligado or Inhofe's hold but was in response to O'Rielly not supporting the Trump administration's petition that the FCC re-examine Section 230," SpaceNews reported.

"I understand this nom[ination] was pulled because [O'Rielly] wasn't supportive of Trump's illegal & unconstitutional request that FCC interpret Section 230," Gigi Sohn, a consumer advocate who was an FCC official during the Obama administration, wrote on Twitter. Sohn and O'Rielly have repeatedly taken opposing positions on controversial FCC decisions such as net neutrality rules, but Sohn wrote, "Give Mike props—he stuck to his principles even as it may have cost him another term as Commissioner."

https://arstechnica.com/?p=1696356