FBI nabs Nigerian business scammer who allegedly cost victims millions



Enlarge / Ray “Hushpuppi” Abbas poses in front of a private jet in a 2019 Instagram photo. “It’s a different type of GLOW and STANDARD when you start hopping out of Rolls Royces to catch a Jet just to attend fashion shows in a different continent,” he wrote. “Your smile begin to be bright just as the sun.”

reader comments

24 with 20 posters participating

Share this story

The US government has gained custody of a Nigerian man who is

accused of participating in a massive fraud and money laundering operation. The defendant, Ray “Hushpuppi” Abbas, has amassed 2.4 million followers on Instagram, where he flaunts his access to luxury cars, designer clothing, and private jets. The feds say that he gained this wealth by defrauding banks, law firms, and other businesses out of millions of dollars. He was arrested last month by authorities in the United Arab Emirates, where he had been living.

The FBI’s criminal complaint details how the government obtained a wealth of information tying Abbas to his alleged crimes. Abbas was an avid user of American technology platforms, including Instagram, Gmail, iCloud, and Snapchat. Accounts on these platforms were all registered using a handful of common email addresses and phone numbers. Abbas’s main email account—rayhushpuppi@gmail.com—included a copy of Abbas’s lease at a luxury hotel in Dubai and scans of various government-issued photo IDs under Abbas’ name.

Abbas is accused of participating in a number of “business email compromise” scams. By posing as trusted employees or customers of a target organization, Abbas and his fellow fraudsters allegedly tricked employees into sending large sums to bank accounts they controlled.

In one incident detailed in the FBI complaint, Abbas and two co-conspirators allegedly defrauded a law firm in New York state. The firm needed to wire more than $900,000 on behalf of a client who was closing a real estate deal. The fraudsters tricked a paralegal into sending email to a fake address purporting to belong to Citizens Bank. The fraudsters responded by faxing instructions for wiring cash to an account they controlled. A law firm employee attempted to “confirm” the instructions by calling the phone number on the form—but that number was controlled by the scammers. By the time the law firm noticed the funds hadn’t made it to the intended destination account, it was too late to get it back.

In another incident, an overseas bank “suffered a computer intrusion and cyber-heist in which approximately €13 million ($14.7 million) was fraudulently wired” from the victim bank to bank accounts in other countries.

Bank accounts

The FBI hasn’t accused Abbas of personally infiltrating victim companies. Rather, his alleged role was to find bank accounts that could accept millions of dollars in stolen cash without raising red flags. Abbas provided co-conspirators with wire information for accounts in Romania, Bulgaria, Dubai, Mexico, and elsewhere.

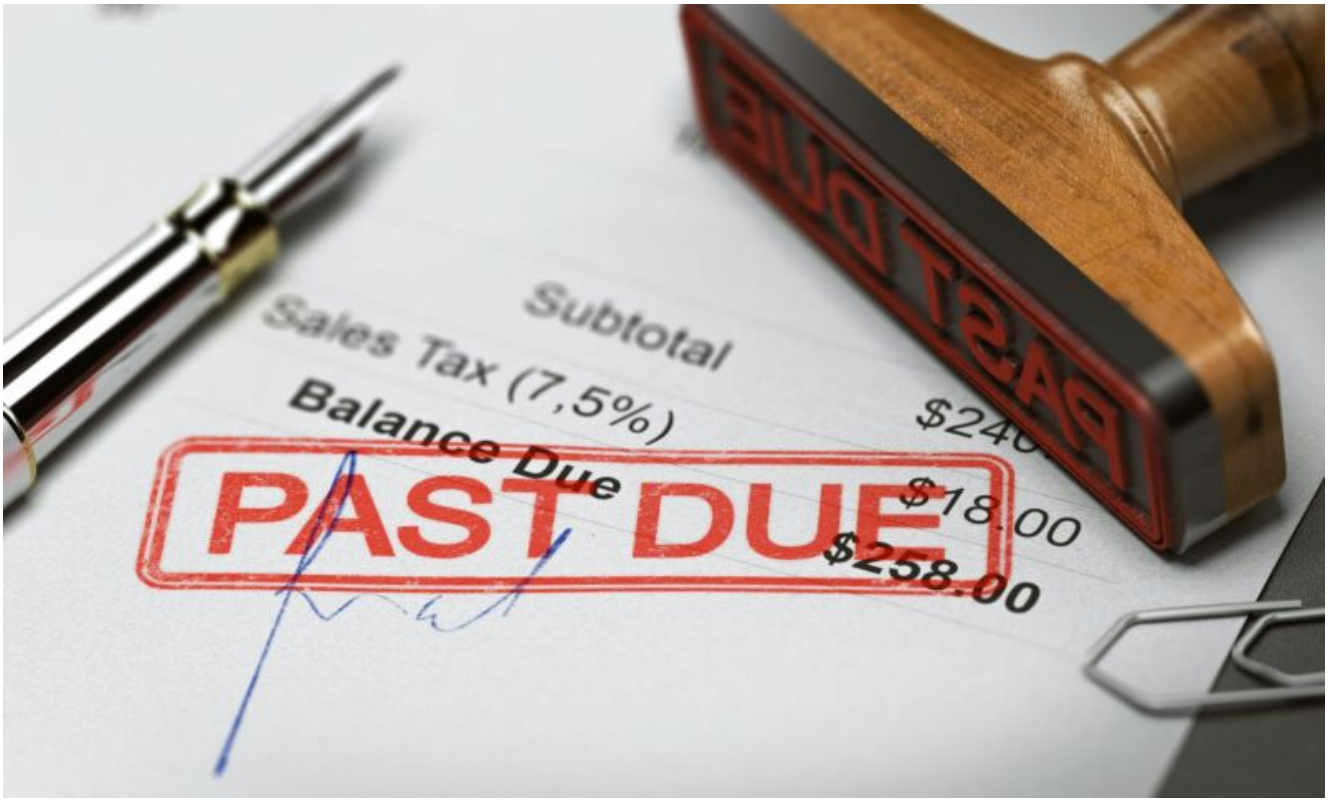
The FBI was able to obtain minute-by-minute documentation of Abbas’ participation in these schemes via their text messages and other online communications. One key source: the FBI apparently gained access to the iPhone of an Abbas associate who was arrested at a US airport last October.

The Justice Department says that, after arresting Abbas last month, UAE authorities expelled him to the United States, where he arrived on Thursday. He made his initial court appearance in Chicago on Friday. The FBI says that business-email compromise scams—by Abbas and others—cost companies at least $1.7 billion in 2019 alone.

https://arstechnica.com/?p=1689658

Supreme Court strikes down

2015 law allowing robocalls by debt collectors



Getty Images | Olivier Le Moal

reader comments

101 with 74 posters participating

Share this story

The US Supreme Court today struck down a provision in US law that let debt collectors make robocalls to cell phones, ruling that the law violates the First Amendment by favoring debt-collection speech over other speech.

The Telephone Consumer Protection Act (TCPA) of 1991 prohibits "almost all robocalls to cell phones," but Congress in 2015 amended the law to add "a new government-debt exception that allows robocalls made solely to collect a debt owed to or guaranteed by the United States," the Supreme Court noted in

today’s ruling. The opinion was written by Justice Brett Kavanaugh.

“As the Government concedes, the robocall restriction with the government-debt exception cannot satisfy strict scrutiny,” the ruling said. “The Government has not sufficiently justified the differentiation between government-debt collection speech and other important categories of robocall speech, such as political speech, issue advocacy, and the like.” Government-backed loans affected by the ruling include student loans, home mortgages, veterans’ loans, farm loans, and business loans.

The case began when the American Association of Political Consultants and three other organizations that “make calls to citizens to discuss candidates and issues, solicit donations, conduct polls, and get out the vote” sought the invalidation of the entire TCPA, the ruling said:

> *Plaintiffs in this case are political and nonprofit organizations that want to make political robocalls to cell phones. Invoking the First Amendment, they argue that the 2015 government-debt exception unconstitutionally favors debt-collection speech over political and other speech. As relief from that unconstitutional law, they urge us to invalidate the entire 1991 robocall restriction, rather than simply invalidating the 2015 government-debt exception.*

Six of the nine justices determined that the 2015 update to the law “impermissibly favored debt-collection speech over political and other speech, in violation of the First Amendment,” the ruling said. But instead of striking down the whole law, the Supreme Court found that the TCPA can be enforced without the exception for debt collectors. That’s partly because the “TCPA is part of the Communications Act, which has contained an express severability clause since 1934.” But even if that clause didn’t exist, “the presumption

of severability would still apply," the court said.

"The remainder of the law is capable of functioning independently and would be fully operative as a law. Severing this relatively narrow exception to the broad robocall restriction fully cures the First Amendment unequal treatment problem and does not raise any other constitutional problems," the high court said. Because of traditional severability principles, "the 2015 government-debt exception must be invalidated and severed from the remainder of the statute," the court said.

While plaintiffs didn't get what they asked for, Americans now have legal protection against robocalls from debt collectors. "As a result, plaintiffs still may not make political robocalls to cell phones, but their speech is now treated equally with debt-collection speech," the Supreme Court said.

The plaintiffs in the case did not challenge the TCPA's ban on robocalls to home phones. The Federal Communications Commission enforces the law but is largely ineffective at collecting on fines issued to violators.

Court "side[d] with American consumers"

Today's Supreme Court ruling upheld a previous ruling by the US Court of Appeals for the Fourth Circuit. That Fourth Circuit judgment overturned a District Court ruling that upheld the debt-collection provision "because of the Government's compelling interest in collecting debt," the Supreme Court ruling said.

Sen. Ed Markey (D-Mass.) and Rep. Anna Eshoo (D-Calif.) praised the court's decision today. "The court rightly found that government debt collectors aren't entitled to a special exception to the TCPA's ban on robocalling," Markey and Eshoo

said in a joint statement. “We applaud the court’s decision to side with American consumers, protect our right to privacy from these abusive calls, deter countless scams that target our most vulnerable populations, and ensure that our phones will remain usable.”

Noting that the court allowed the TCPA to stand on its own without the debt-collection exception, Markey and Eshoo said that “today’s decision preserves the TCPA’s ability to protect Americans from countless unwanted robocalls every year, every day, and indeed every hour and minute.” Markey was one of the authors of the 1991 law.

FCC Chairman Ajit Pai also welcomed the ruling, saying that “the Court found that the last Administration’s attempt to create a special exemption for favored debt collectors was not only bad policy but unconstitutional.”

How each justice ruled

Kavanaugh was joined by Chief Justice John Roberts, Clarence Thomas, and Samuel Alito in finding that “the robocall restriction with the government-debt exception is content-based” and is “subject to strict scrutiny.” Content-based restrictions on speech have to pass greater legal scrutiny than content-neutral restrictions.

“The Government’s stated justification for the government-debt exception is collecting government debt,” the Kavanaugh-written opinion said. “Although collecting government debt is no doubt a worthy goal, the Government concedes that it has not sufficiently justified the differentiation between government-debt collection speech and other important categories of robocall speech, such as political speech, charitable fundraising, issue advocacy, commercial advertising, and the like.”

Justice Sonia Sotomayor concurred with the judgment, finding

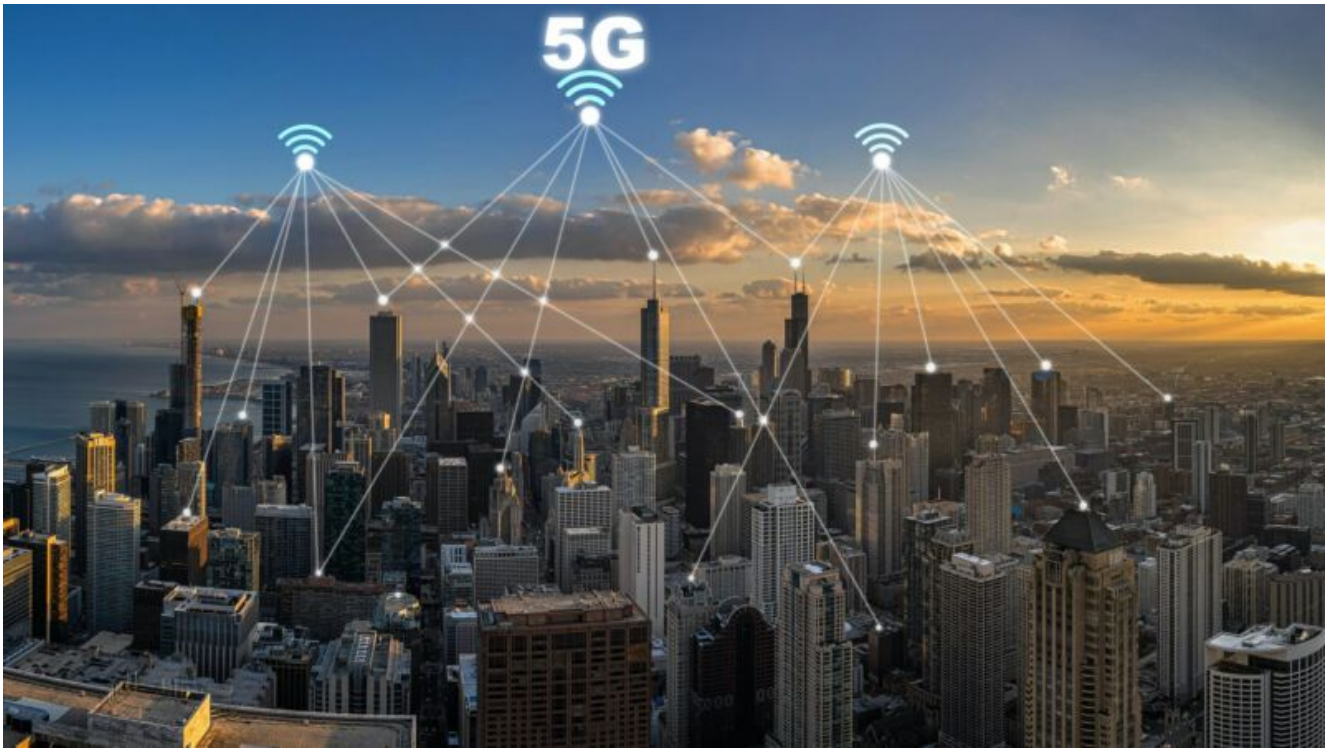
that the debt-collection provision “fails intermediate scrutiny because it is not ‘narrowly tailored to serve a significant governmental interest.'” Justice Neil Gorsuch found that “the TCPA’s rule against cellphone robocalls is a content-based restriction that fails strict scrutiny,” but rejected the severability argument and said “the plaintiffs are entitled to an injunction preventing [the TCPA’s] enforcement against them.”

Meanwhile, “Justice [Stephen] Breyer, joined by Justice [Ruth Bader] Ginsburg and Justice [Elena] Kagan, would have upheld the government-debt exception, but given the contrary majority view, agreed that the provision is severable from the rest of the statute,” the ruling said.

The TCPA generally bans unsolicited prerecorded telemarketing calls but explicitly provides an exemption for tax-exempt nonprofit organizations.

https://arstechnica.com/?p=1689578

5G was going to unite the world—instead it’s tearing us apart



reader comments

67 with 55 posters participating

Share this story

The world came together to build 5G. Now the next-generation wireless technology is pulling the world apart.

The latest version of the 5G technical specifications, expected Friday, adds features for connecting autonomous cars, intelligent factories, and Internet-of-things devices to crazy-fast 5G networks. The blueprints reflect a global effort to develop the technology, with contributions from more than a dozen companies from Europe, the US, and Asia.

And yet, 5G is also pulling nations apart—with the United States and China anchoring the tug-of-war. Tensions between Washington and Beijing over trade, human rights, the handling of COVID-19, and Chinese misinformation are escalating global divisions around the deployment of 5G. A growing number of countries are aligning with either a Western or a Chinese version of the tech.

“National security and commercial interests are all entangled, and it’s very hard to separate them,” says Scott Wallsten, president of the Technology Policy Institute, a think tank.

The way 5G was created, and the way it is now being deployed, captures an ongoing conundrum for Western countries—how to balance healthy competition and collaboration with national interests and the rise of China.

The 5G dispute centers on Huawei, which is arguably China’s most important tech company and has a dominant position in networking equipment, a big smartphone business, and increasingly sophisticated chips. The company is accused of stealing technology and of having close ties to the Chinese government that might enable cyber-espionage. It has become a symbol of China’s ambitions to dominate the technology, through innovation as well as nefarious means.

The US and some allies, including Australia, New Zealand, Japan, and Taiwan, have banned Huawei and other Chinese telcos like ZTE from their networks. Other nations have balked at US-led efforts to keep Huawei and other Chinese firms out of the picture. Argentina, Brazil, Russia, the Philippines, and Thailand all welcome China’s 5G tech.

A key question is how this bifurcation will affect the workings of a standard that was meant to be open and global. “We risk further fragmenting the Internet and the way different networks connect to each other,” says Wallsten.

Even if 5G was meant to be a truly global communications standard, the technical plans reflect shifting national strengths and resulting tensions.

The 5G standards outline plans for insanely fast wireless speeds of up to 1GB per second—50 times faster than the

average US broadband connection—with few delays. Think playing high-end games without any lag or robots that feed on artificial intelligence hosted in the cloud. And, of course, 5G is expected to inspire innovations and businesses that could change the technology landscape. By various estimates, the technology could generate several trillion dollars for the global economy over the next couple of decades. It’s no surprise that every country wants a piece of the action.

Collaboration

The technical specifications for 5G are developed by the 3rd Generation Partnership Project (3GPP), a coalition of standards organizations from the US, Europe, China, Japan, India, and South Korea. The group is putting the finishing touches on Version 16 of the 5G specs, which will add features that let devices hop among a wider range of wireless spectrum as well as offer high-precision positioning, vehicle-to-vehicle connectivity, and more reliable, virtually instantaneous communications, crucial for industrial uses.

Many companies have contributed to the drafting of 5G, but the standard reflects a shift from US and European tech to Chinese compared with 4G, the previous standard. An analysis of contributions to 3GPP specifications, published in August 2019 by IHS Markit, found that Chinese firms contributed approximately 59 percent of the standards, with Huawei accounting for the most of those. The standards for 4G were led by European and American firms.

“The US wrote 4G,” says Charles Clancy, vice president for intelligence programs at MITRE, a nonprofit that manages US research projects. “In the meantime, through government subsidies and cyber theft of competitors’ intellectual property, Huawei became the global leader while nobody was watching,” says Clancy, who has studied 5G security. “They slowly took control of the standards groups, and China wrote

5G.” Huawei declined to comment.

It remains hard to gauge how much China stands to gain from its role shaping the standards—or how much the US stands to lose. Defining technical standards can give hardware makers an edge in developing products that use the standards. Huawei has also been accused of making its hardware difficult to combine with other gear. A November report from the Center for New American Security warns that 5G promises to have such broad uses that the US could suffer economically and militarily if it lets China get too far ahead.

Competition

The competition can get tricky, however. Last month, the US government clarified a rule allowing US companies to work with Huawei on technical standards, after previous versions apparently caused US firms to lessen their involvement in standard-shaping.

Despite the complexities, many countries are falling in line with the US. Secretary of State Mike Pompeo declared last week that the “tide is turning against Huawei” and hailed “clean telcos” in India, France, Australia, South Korea, and the UK that are spurning the Chinese company’s tech. On the same day, the government of Singapore chose Ericsson of Sweden and Nokia of Finland, instead of Huawei, to install its national 5G network.

Some countries seem keen to take advantage of the division between the US and China. A day after Singapore made its choice, Japan’s dominant telco NTT Docomo took a 5 percent stake in hardware maker NEC, and the companies outlined plans to compete globally in 5G. The Japanese government also signalled plans to push a Japanese version of the technology.

5G has inspired new coalitions among nations, including the D-10, a coalition of democratic nations proposed by the UK

that would collaborate on technologies like 5G as well as global supply chains.

Samm Sacks, a cybersecurity policy and China digital economy fellow at New America, notes that the US is increasingly taking a more offensive approach to competition with China in areas such as artificial intelligence, chip development, and 5G by proposing more investment in chipmaking technology and promoting open communications standards.

This story first appeared on wired.com.

https://arstechnica.com/?p=1689260

Schools already struggled with cybersecurity. Then came COVID-19



Enlarge / “School” is probably going to look something like this for a whole lot of families in the coming weeks.

reader comments

26 with 19 posters participating

Share this story

Covid-19 Coverage

View more stories

This time last year, Jaggar Henry was enjoying the summer like so many other teens. The 17-year-old had a job, was hanging out with friends on the weekends, and was just generally spending a lot of time online. But then, at the end of July, Henry combed his hair, donned a slightly oversized Oxford shirt, and appeared before his school district’s board in Polk County, Florida—one of the larger school districts in the

United States—to outline a slew of security flaws he had found in its digital systems. His presentation was the culmination of months of work and focused on software used by more than 100,000 students.

Those vulnerabilities have been fixed, but Henry, who now works full time on education technology, says that his experience illustrates the challenges facing school districts across the United States—and a problem that's grown more acute in the wake of COVID-19.

The coronavirus pandemic has had major cybersecurity implications around the world. Tailored phishing attacks and contact-tracing scams prey on fear and uncertainty. Fraudsters are targeting economic relief and unemployment payments. The stakes are higher than ever for ransomware attacks that target health care providers and other critical infrastructure. For businesses, the transition to remote work has created new exposures and magnified existing ones.

School districts in the United States already had significant cybersecurity shortcomings. They often lack dedicated funding and skilled personnel to continuously vet and improve cybersecurity defenses. As a result, many schools make basic system-setup errors or leave old vulnerabilities unpatched—essentially propping a door open for hackers and scammers. Schools and students also face potential exposure from third-party education-technology firms that fail to adequately secure data in their platforms.

The pandemic amplified these risks, as school districts around the country transitioned to distance learning in the spring. Suddenly, millions of teachers and students relied on video chat software, lesson portals, digital message boards, and other online tools. If these systems are set up without proper

authentication and controls, any of them can potentially become vectors for attack. And tools to access school networks remotely, including VPNs and Remote Desktop Protocol, can be abused by attackers to gain unauthorized access to sensitive systems. Last week, the Federal Bureau of Investigation issued a security alert about the threat of ransomware to schools amidst the COVID-19 crisis. “K-12 institutions have limited resources to dedicate to network defense, leaving them vulnerable to cyber attacks,” the FBI warned, according to a ZDNet report.

In the past 30 days, more than 4.7 million malware incidents were detected in the education industry broadly worldwide, according to Microsoft’s Global Threat Activity tracker—more than 60 percent of all the corporate and institutional malware incidents reported during that time. The next most affected sector is what Microsoft calls “business and professional services,” with fewer than 1 million incidents.

“Ill-equipped”

“Many schools are ill-equipped to securely migrate to a completely digital learning experience, so it comes as absolutely no surprise that these vulnerabilities are so prevalent,” says Henry. “School districts are scrambling, and threat actors know this.”

Henry says he first became interested in probing his own school’s digital systems after hearing how much they cost. Polk County is the seventh-largest school district in Florida, with more than 100,000 students, and in recent years it had been spending millions of dollars to develop an enrollment system called Delta and to contract for a new “Student Information System” from an outside vendor. The school board reportedly made the switch with security in mind. Henry first reported flaws in the school’s new SIS implementation in September 2018, though. The following March, he found data

exposed in Delta. The application accessed students' identifying information, like Social Security numbers, through an application programming interface. Henry realized that he could manipulate the API to spit out other students' results simply by changing an internal reference ID number the app used to keep track of each student.

Another issue Henry found was in the way Polk County used Microsoft SharePoint platform, a collaboration and storage tool, to manage data. He noticed that students and teachers were lumped together in a Sharepoint "user group" and had all been granted the same access to files stored in the system. This meant that students could access anything on the Sharepoint, including each others' data. One file was labeled as containing student usernames and passwords and was simply an unlocked, plaintext spreadsheet of student login credentials for school accounts.

Polk County Schools did not return a request for comment on Henry's research. At the July 2019 meeting where Henry shared his findings, though, members of the school board appeared to support his work. "I've directed him multiple times to our IT staff," Billy Townsend, the school board representative for Polk County's District 1, said. "I think he's done some very useful things, from what I understand. I think we should take seriously what he's saying."

"Nobody else is looking"

Henry also found and reported similar vulnerabilities in the systems of two private Florida universities last year. He says that making all of these discoveries while he was still a student motivated him to pursue a career in ed-tech cybersecurity.

"When I took a look, there was so much that was vulnerable—just a stupid amount of vulnerability," Henry says. "It doesn't feel good. When you participate in a capture-the-

flag hacker competition or do a cool bug bounty, it feels good to find stuff, but you see these flaws in education systems and there's nothing to be proud of as a researcher. You changed a number or you just looked! I'm not some genius. It's just very obvious that nobody else is looking."

After some especially dramatic cyberattacks against schools in the fall, including multiple situations where districts had to cancel class because of ransomware attacks, researchers say that there started to be momentum toward making cybersecurity a priority in school systems around the country. But Doug Levin, founder of the consulting firm EdTech Strategies, which compiles data on K-12 cybersecurity incidents, says all of that ground to a halt when the COVID-19 pandemic hit.

"Suddenly everything shifted on a dime," Levin says, recalling how schools raced to set up infrastructure for online learning en masse. "It went into that mode where everything is built with rubber bands and toothpicks. Get everyone working and learning remotely, distribute devices to students, connect to local printers, deal with forgotten passwords, whatever. People should be concerned about the technical decisions they were making. And even with a bit more time to plan for the fall, it's all still very fluid."

Undercounts

There's no single, comprehensive source of reporting on K-12 digital security incidents in the US. Levin created the Cyber Incident Map to track as many publicly disclosed attacks as possible—compiled from legal disclosures, news reports, and research findings. But the tracker likely undercounts actual total incidents by a significant margin, since so many are kept under wraps and never go public.

In the past three months, Levin has been surprised to see a decrease in the number of public accounts of K-12 cyber attacks, though they're certainly not gone altogether. It's

unclear if this actually represents a downtick in the number of incidents or whether other factors are at play. Levin also points out that there may be a new digital-infection spike in the fall when students, teachers, and administrators physically go back to school and plug their devices into hardwired networks for the first time in months.

While the pandemic has fueled new exposures, it has also simply accelerated a digitization that was already in progress across K-12 education—a phenomenon seen in virtually every industry. Given the cracks that already existed in schools' digital defenses, it's more vital than ever to take precautions now.

This story first appeared on wired.com.

https://arstechnica.com/?p=1689253

Commerce Inspector General says "Sharpiegate" report being blocked

Enlarge / Commerce Secretary Wilbur Ross.

reader comments

10 with 10 posters participating

Share this story

Last month, we covered the results of a NOAA investigation into scientific integrity violations associated with its handling of President Donald Trump's self-inflicted hurricane controversy.

The problems started when Trump incorrectly tweeted that Alabama was likely going to be impacted by Hurricane Dorian. After seeing an influx of questions, the Birmingham National Weather Service office tweeted a clarification. Rather than simply correcting the mistake, the White House insisted that the President was right, an insistence that eventually led to his marker-amended forecast map, presented from the Oval Office.

NOAA's issue was that its leadership released an unsigned statement that sided with President Trump, criticizing the Birmingham office for speaking "in absolute terms that were inconsistent with probabilities from the best forecast products available at the time."

From NOAA to Commerce

NOAA's scientific integrity officer commissioned an investigation into that statement, concluding that Acting Administrator Neil Jacobs and Director of Communications Julie Kay Roberts had violated agency rules in releasing that statement. But the investigation also concluded that the statement had actually been directed by Commerce Department leadership—none of whom were willing to answer questions from the NOAA investigators.

Enter the Commerce Department Inspector General, who started a parallel investigation. On Monday, agency Inspector General Peggy Gustafson posted a memo summarizing her conclusions. Curiously, the memo—dated June 26—said that the full report was set to be posted at the same time on Monday. Yet the full

report wasn't there, and the memo itself contained several redactions "pending privilege review."

On Wednesday night, Gustafson posted a second memo with the subject, "The Department Is Actively Preventing OIG from Completing an Evaluation." In it, Gustafson effectively alleges that the office of Commerce Secretary Wilbur Ross is stonewalling the report's release.

The summary memo listed four primary conclusions:

> *I. The Department led a flawed process that discounted NOAA participation.*
>
> *II. The Department required NOAA to issue a Statement that did not further NOAA's or the National Weather Service's interests.*
>
> *III. The Department failed to account for the public safety intent of the National Weather Service Birmingham tweet and the distinction between physical science and social science messaging.*
>
> *IV. One NOAA employee deleted relevant text messages, and the Department's federal records guidance is outdated.*

According to the report NOAA commissioned, it was Julie Kay Roberts—the Director of Communications who featured in NOAA's report—who had deleted text messages.

The second memo from Commerce Inspector General Peggy Gustafson says that Commerce leadership agreed to review her report within 48 hours, identifying any specific statements it felt needed to be redacted. But Gustafson says that the Secretary's office is now upset that the report references information in evidentiary appendices that it had previously asked to be redacted. Gustafson writes, "This position is without merit as it suggests that the Department has a role in how OIG drafts its reports and what evidence is relied upon.

On the contrary, the Department has no part in determining how or when OIG conducts its oversight work or structures its reports. To expect otherwise is contrary to the IG Act and an unacceptable intrusion on OIG's independence."

Gustafson says that leadership is now refusing to identify specific statements that it wants redacted, leaving the final report in limbo. She continues, "Notably, communications were consistently collegial, until OIG transmitted the final report for a privilege review and subsequent issuance of the final report to you. This tone shift appears to be directly linked to the content of our report and the findings of responsibility of the high-level individuals involved."

In other words, Gustafson thinks that, upon finding that the report concluded that senior officials in Commerce were responsible for the problems, said officials stopped cooperating. The memo requests that the Secretary's office provide its specific redaction requests by July 9 so the report can be released.

https://arstechnica.com/?p=1689199

Police infiltrate encrypted phones, arrest hundreds in organized crime bust

Enlarge / It is not specified if Encrochat users were required to stand in silhouette or otherwise apply film-noir style lighting while using their encrypted phones to do crime.

reader comments

46 with 32 posters participating

Share this story

Almost 750 individuals in the UK have been arrested so far after an international coalition of law enforcement agencies infiltrated an encrypted chat platform in which the suspects openly discussed murder, arranged hits, illegal drug purchases, gun sales, and other alleged crimes.

The UK's National Crime Agency (NCA) today announced the results of an investigation it dubbed Operation Venetic. UK agencies, taken together, have to date arrested 746 suspects and seized 77 guns, two metric tons of drugs, 28 million illicit pills, 55 "high value" cars, and more than £54 million ($67.4 million) in cash.

The arrests followed a breakthrough into an encrypted communications platform, Encrochat, used widely in the European underground. "The infiltration of this command and control communication platform for the UK's criminal marketplace is like having an inside person in every top organized crime group in the country," NCA Director of Investigations Nikki Holland said in a written statement. "This is the broadest and deepest ever UK operation into serious organized crime."

The investigation began in France, where it eventually was called "Emma 95," in 2017, according to Europol, the joint European Union law enforcement agency. It then spread to the Netherlands under the code name "Lamont" and eventually came to the UK. Users in Sweden and Norway were also implicated in drug trafficking and other organized crime, Europol said.

French authorities declined to disclose publicly the details of their investigations or the results so far, but Dutch authorities said they have arrested more than 100 suspects and

seized more than 8,000kg of cocaine, 1,200kg of crystal meth, dozens of guns and luxury cars, and almost €20 million ($22.5 million) in cash.

No backdoor needed

The suspects were all communicating through Encrochat, an encrypted service requiring specialized phones to operate. As Europol described it:

> *Encrochat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port)*

The investigators who found a way in to the platform didn't try to break the encryption in any way. Instead, they went for the devices, installing malware to allow them to read messages before they were sent. Vice Motherboard reviewed a trove of leaked documents and spoke with law enforcement, Encrochat, and criminals to report in depth what happened.

Encrochat "is highly secretive and does not operate like a normal technology company," Motherboard observed. While "someone in control of a company email address" told the site that it is a legitimate firm with customers in 140 nations, criminal-affiliated sources said that a whole lot of Encrochat customers are doing something illegal.

The phones themselves are modified Android devices, Motherboard explains, including a model called the BQ Aquaris X2 that's made by a Spanish firm. Encrochat physically removed GPS, camera, and microphone capabilities from the handsets, so

users could not be recorded or traced through them. The company also installed dual operating systems on each device (standard Android as well as the Encrochat system) so the phone could masquerade as a normal device. The devices also boasted a feature allowing them to be wiped completely if the user entered a certain PIN.

Not user error

In May, Motherboard reports, some Encrochat users started to have problems with that wipe feature. At first, Encrochat assumed it was user error or a rogue bug. In May, the company got its hands on one of the X2 devices with the problem and discovered the issue was not user error. Instead, it was malware that not only prevented the wipe but also recorded screen lock passcodes and cloned application data.

Encrochat pushed an update, but the devices were almost immediately struck again, and the new malware could not only record lock screen passcodes—it could also alter them. After attempting several ways to work around the attack by halting SIM service, Encrochat determined the attack was likely from law enforcement and decided to shut down. On June 13, it warned customers: “Today we had our domain seized illegally by government entities(s). They repurposed our domain to launch an attack to compromise the carbon units.”

The company estimated about 50 percent of units in Europe were affected. “Due to the level of sophistication of the attack and the malware code, we can no longer guarantee the security of your device,” Encrochat added, advising users to power off and physically dispose of their phones.

As has become clear, though, the shutdown came too late, and law enforcement agencies already had access to an enormous trove of data.

One source told Motherboard the mass arrests seem to have had

their desired effect and told the site that bulk purchases of drugs had become significantly harder because “everybody’s going to ground.” Still, the quiet may not last: competitors are not only moving to fill the space, but they’re offering discounts to onetime Encrochat users who may now be looking for a new platform.

https://arstechnica.com/?p=1689071

House OKs $100B broadband plan with $50 monthly discounts for poor people

reader comments

45 with 35 posters participating

Share this story

The US House of Representatives yesterday approved $100 billion worth of broadband funding as part of a $1.5 trillion infrastructure bill.

The broadband portion is modeled on the Democrats’ “universal fiber” plan we wrote about last week. The plan includes $80 billion in fiscal year 2021, money that the Federal Communications Commission would use to fund high-speed broadband projects in unserved and underserved areas. Funded projects would have to provide 100Mbps download and upload

speeds, along with low latencies, conditions that would spur fiber-to-the-home development.

The bill has additional money for broadband-deployment loans, grants for states to pursue digital-inclusion projects, Wi-Fi on school buses, and network equipment for schools and libraries. It also includes a $9 billion Broadband Connectivity Fund to provide $50 monthly discounts for low-income broadband users, and $75 monthly discounts for low-income households in Tribal lands. The broadband portions of the infrastructure bill are in this set of amendments.

The bill also has a Dig Once requirement that says fiber or fiber conduit must be installed “as part of any covered highway construction project” in states that receive federal highway funding. The bill would also overturn state laws that “prohibit or have the effect of prohibiting” municipal broadband networks.

“This legislation takes a comprehensive approach towards closing the digital divide by focusing on deployment and affordability,” Senior Policy Counsel Jenna Leventoff of consumer-advocacy group Public Knowledge said. “Ensuring that consumers not only have the ability to purchase broadband, but also the ability to afford it is key for narrowing our nation’s staggering digital divide.”

Party-line vote

The infrastructure bill isn’t likely to pass as currently written in the Republican-controlled Senate, but it’s possible at least some of the broadband portions will become law in a compromise. The overall bill passed by a vote of 233-188, while the broadband provisions were part of a set of amendments that passed in a 234-178 vote. “While the party-line vote on the full bill is a fact of our current politics, no one should make the mistake of thinking the broadband provisions are partisan,” Free Press General Counsel Matt Wood

said. “People in cities and rural areas alike need better broadband at better prices, no matter their party or politics. The Moving Forward Act recognizes and addresses the needs of communities most often left out of congressional debates on communications policy.”

The legislation also recognizes “that the vast majority of people who are disconnected today are offline because of the high price of Internet services that are physically available to them but out of reach financially,” Wood said. “This dilemma disproportionately impacts Black and Brown people, poorer communities and other groups hit hardest by the pandemic. Lacking an Internet connection during this health crisis exacerbates existing economic inequities and deepens digital divides.”

The House-approved package is one of several pending attempts to close broadband gaps. Another Democratic bill would provide $50 monthly broadband credits ($75 in Tribal lands) for people who have been laid off or furloughed during the pandemic.

https://arstechnica.com/?p=1689099

Tesla stock leaps again on unexpectedly strong delivery numbers

Enlarge / A Tesla facility in Lathrop, CA.
Andrei Stanescu / Getty

reader comments

181 with 89 posters participating, including story author

Share this story

Tesla has surprised Wall Street again with better-than-expected delivery numbers. The electric carmaker delivered 90,650 vehicles in the second quarter of 2020, up slightly from the 88,400 vehicles delivered in the first quarter. This despite the fact that Tesla's main factory in Fremont, California, was shut down by county officials for the first half of the quarter.

Tesla's stock leapt at the news. After closing at a record high of $1,120 yesterday, Tesla's shares rose above $1,200 in pre-market trading on Thursday morning.

While Tesla's Q2 deliveries were up from the previous quarter, they're down slightly from the 95,200 vehicles produced in the second quarter of 2019. Tesla also delivered more cars in Q3 and Q4 of 2019 than it did last quarter. That presumably reflects the effects of the coronavirus over the last two quarters, as well as the phaseout of the federal tax credit for purchasing a Tesla. The credit fell by half on June 30, 2019 and phased out completely on December 31.

Tesla's 5 percent decline in year-over-year deliveries compares favorably to other carmakers. GM suffered a 34 percent year-over-year sales decline in the second quarter of 2020. Fiat Chrysler saw sales fall 39 percent year over year. Other carmakers that have reported so far have seen year-over-year declines ranging between 9 percent and 58 percent.

Tesla produced 82,272 vehicles in the second quarter, 8,400 fewer than it delivered—which means that Tesla has been drawing down inventories built up prior to the pandemic. Tesla says it has now ramped up production to pre-pandemic levels, setting the stage for growth in Q3.

Model S and Model X sales continue to slump

In 2018, Tesla delivered almost 25,000 Model S and Model X (combined) per quarter. In 2019, this fell to around 17,000.

In the first quarter of 2020, Model S and Model X deliveries were at 12,200. In the second quarter, the number was 10,600.

Cooling interest in these high-end cars likely reflects the fact that Tesla hasn’t done a major refresh of either model in several years. That makes it hard for consumers to justify paying a big premium over the newer Model 3 and Model Y, which accounted for the bulk of Tesla’s sales last quarter.

https://arstechnica.com/?p=1689038

Small ISPs “stunned” by FCC move to ban Huawei/ZTE gear during pandemic

Enlarge / Huawei sign displayed at CES 2020 in Las Vegas on Wednesday, Jan. 8, 2020.

reader comments

69 with 51 posters participating

Share this story

Small Internet service providers are “stunned” that the Federal Communications Commission is enforcing a ban on Huawei and ZTE network gear during the ongoing pandemic.

The FCC already voted unanimously in November 2019 to ban Huawei and ZTE equipment in projects paid for by the commission’s Universal Service Fund (USF). But the ban, inspired by fears that the Chinese vendors’ equipment poses national security risks, is just now coming into effect, with the FCC announcing yesterday that USF money “may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by these suppliers.”

The Rural Wireless Association (RWA), a trade group that represents ISPs that serve fewer than 100,000 subscribers each, said yesterday it is “stunned by [the] FCC’s decision to immediately bar use of USF funds on Huawei and ZTE equipment and services during a time when it is critical to keep rural Americans connected.”

The RWA statement said:

> *As a result, rural carriers who have deployed Huawei or ZTE equipment or services in their networks will now lack the ability to support their critical networks that are serving hundreds of thousands of rural Americans and those traveling through rural America. Given the difficulty in demonstrating where specifically their USF support is being utilized in their networks, this puts rural carriers in a precarious situation while they strive to offer extended payment terms for their customers as requested by FCC Chairman [Ajit] Pai, adjust to the fallout of the T-Mobile/Sprint merger, and continue to keep rural Americans connected to broadband and telephone services during the COVID-19 pandemic.*

The FCC's public notice said ISPs "may seek a waiver of this prohibition if necessary," but the RWA said ISPs should have been given more time to seek waivers. "RWA members appreciate the opportunity to submit waivers of this prohibition but ask the commission to give them sufficient time to submit such waivers before pulling away their USF support which is scheduled to start tomorrow, July 1," the group said yesterday.

FCC defends ban but needs funding

The FCC said its ban targets Huawei and ZTE "because of their substantial ties to the Chinese government, Chinese law requiring them to assist in espionage activities, known cybersecurity risks and vulnerabilities in their equipment, and ongoing Congressional and Executive Branch concern about this equipment."

"We cannot and will not allow the Chinese Communist Party to exploit network vulnerabilities and compromise our critical communications infrastructure," Pai said, calling the companies' gear a risk "to our 5G future."

The ban has support from Pai's Republican majority and the FCC's Democrats. Democratic Commissioner Geoffrey Starks said that yesterday's action "will help secure our networks against new threats from Huawei and ZTE equipment" and that the FCC "must not… lose sight of the untrustworthy equipment already in place."

But Starks said Congress has not yet provided funding to help ISPs replace Huawei and ZTE network gear with other companies' equipment:

> *Funding is the missing piece. Congress recognized in the* ***Secure and Trusted Communications Networks Act*** *that many carriers will need support to transition away from untrustworthy equipment, but it still has not appropriated*

> *funding for replacements. I look forward to working with Congress and my colleagues to ensure there are sufficient funds to get the job done.*

The legislation Starks referred to became law in March and says that $1 billion shall be provided in "reimbursement funds to remove, replace, or dispose of any covered communications equipment or service." However, the FCC said in a recent public notice that while the "reimbursement program created by the Secure Networks Act appears to require an express appropriation from Congress," the bill itself "does not provide funding for the reimbursement program and states that the program must be 'separate from any federal universal service program established under section 254 of the Communications Act.'" That apparently means the FCC can't use money it already has for Huawei/ZTE replacements and hasn't gotten money it can use for that purpose from Congress.

While ISPs can no longer use USF money to maintain Huawei and ZTE equipment, they technically aren't required to stop using the equipment entirely. But the FCC is considering another plan to require removal of Huawei and ZTE equipment from USF-funded networks that have already been built.

Huawei: FCC offered "no evidence"

When contacted by Ars, a Huawei spokesperson said that "Huawei believes this order is unlawful as the FCC has singled out Huawei based on national security, but it provides no evidence that Huawei poses a security risk. Instead, the FCC simply assumes, based on a mistaken view of Chinese law, that Huawei might come under Chinese government control."

A ZTE filing in February said the company "conducts business only in compliance with all applicable laws where we are operating, including US export and sanctions laws and regulations." We contacted ZTE today about the FCC decision

and will update this story if we get a response.

https://arstechnica.com/?p=1688738

Uncovered: 1,000 phrases that incorrectly trigger Alexa, Siri, and Google Assistant

reader comments

120 with 106 posters participating

Share this story

As Alexa, Google Home, Siri, and other voice assistants have become fixtures in millions of homes, privacy advocates have grown concerned that their near-constant listening to nearby conversations could pose more risk than benefit to users. New research suggests the privacy threat may be greater than previously thought.

The findings demonstrate how common it is for dialog in TV shows and other sources to produce false triggers that cause the devices to turn on, sometimes sending nearby sounds to Amazon, Apple, Google, or other manufacturers. In all, researchers uncovered more than 1,000 word sequences—including those from *Game of Thrones*, *Modern Family*, *House of Cards*, and news broadcasts—that incorrectly trigger the devices.

“The devices are intentionally programmed in a somewhat forgiving manner, because they are supposed to be able to understand their humans,” one of the researchers, Dorothea Kolossa, said. “Therefore, they are more likely to start up once too often rather than not at all.”

That which must not be said

Examples of words or word sequences that provide false triggers include

- Alexa: “unacceptable,” “election,” and “a letter”
- Google Home: “OK, cool,” and “Okay, who is reading”
- Siri: “a city” and “hey jerry”
- Microsoft Cortana: “Montana”

The two videos below show a *GoT* character saying “a letter” and *Modern Family* character uttering “hey Jerry” and activating Alexa and Siri, respectively.

[embedded content]
Accidental Trigger #1 – Alexa – Cloud
[embedded content]
Accidental Trigger #3 – Hey Siri – Cloud
In both cases, the phrases activate the device locally, where algorithms analyze the phrases; after mistakenly concluding that these are likely a wake word, the devices then send the audio to remote servers where more robust checking mechanisms also mistake the words for wake terms. In other cases, the words or phrases trick only the local wake word detection but not algorithms in the cloud.

Unacceptable privacy intrusion

When devices wake, the researchers said, they record a portion of what’s said and transmit it to the manufacturer. The audio may then be transcribed and checked by employees in an attempt to improve word recognition. The result: fragments of

potentially private conversations can end up in the company logs.

The risk to privacy isn't solely theoretical. In 2016, law enforcement authorities investigating a murder subpoenaed Amazon for Alexa data transmitted in the moments leading up to the crime. Last year, The Guardian reported that Apple employees sometimes transcribe sensitive conversations overheard by Siri. They include private discussions between doctors and patients, business deals, seemingly criminal dealings, and sexual encounters.

The research paper, titled "Unacceptable, where is my privacy?," is the product of Lea Schönherr, Maximilian Golla, Jan Wiele, Thorsten Eisenhofer, Dorothea Kolossa, and Thorsten Holz of Ruhr University Bochum and Max Planck Institute for Security and Privacy. In a brief write-up of the findings, they wrote:

> *Our setup was able to identify more than 1,000 sequences that incorrectly trigger smart speakers. For example, we found that depending on the pronunciation, «Alexa» reacts to the words "unacceptable" and "election," while «Google» often triggers to "OK, cool." «Siri» can be fooled by "a city," «Cortana» by "Montana," «Computer» by "Peter," «Amazon» by "and the zone," and «Echo» by "tobacco." See videos with examples of such accidental triggers here.*
>
> *In our paper, we analyze a diverse set of audio sources, explore gender and language biases, and measure the reproducibility of the identified triggers. To better understand accidental triggers, we describe a method to craft them artificially. By reverse-engineering the communication channel of an Amazon Echo, we are able to provide novel insights on how commercial companies deal with such problematic triggers in practice. Finally, we analyze the privacy implications of accidental triggers and discuss potential mechanisms to improve the privacy of smart*

speakers.

The researchers analyzed voice assistants from Amazon, Apple, Google, Microsoft, and Deutsche Telekom, as well as three Chinese models by Xiaomi, Baidu, and Tencent. Results published on Tuesday focused on the first four. Representatives from Amazon, Apple, Google, and Microsoft didn’t immediately respond to a request for comment.

The full paper hasn’t yet been published, and the researchers declined to provide a copy ahead of schedule. The general findings, however, already provide further evidence that voice assistants can intrude on users’ privacy even when people don’t think their devices are listening. For those concerned about the issue, it may make sense to keep voice assistants unplugged, turned off, or blocked from listening except when needed—or to forgo using them at all.

https://arstechnica.com/?p=1688628