COVID-19 spread 4X faster in one Amazon warehouse than local area

Enlarge / An Amazon worker in a fulfillment center in the Orlando area, April 2019.

reader comments

27 with 22 posters participating

Share this story

After eliminating temporary “hazard” pay raises, Amazon is saying “thank you” to its hourly workers with a one-time bonus of $500, while at least one Amazon warehouse has been found to have a COVID-19 rate four times higher than the general population nearby.

Amazon yesterday announced its one-time bonuses for “front-line” employees. Full-time workers in warehouses and Whole Foods stores, as well as full-time delivery drivers, will receive $500. Part-time workers in those roles will get $250, and Amazon Flex drivers who worked 10 hours or more will get $150. Managers on-site in distribution centers or Whole Foods stores will get $1,000, and owners of the third-party firms that handle delivery for Amazon will get $3,000.

The company saw a massive spike in consumer demand as in-person retail shuttered around the nation and the world this spring due to the COVID-19 pandemic. Amazon hired an additional 175,000 employees in its warehouses, logistics, and grocery businesses since early March to meet increased demand. The company also increased wages by $2 in warehouses, to a

minimum of $17 per hour, to get new workers in the door.

But that increase was not guaranteed to be permanent, and it did indeed evaporate after May 30. The $500 that employees who worked full-time for the month of June will receive is equivalent to more than the $2 per hour would have been; for part-time workers, the math is more variable.

Hazard bonus

No employee from any company ever objects to extra cash in hand, but Amazon workers and employee advocates say the money is not enough in the face of the threat from COVID-19, which has hit some warehouses particularly hard.

One Amazon warehouse in Minnesota had an infection rate more than four times higher than the surrounding community, according to an internal memo obtained by Bloomberg. In mid-May, the MSP1 facility outside Minneapolis had a 1.7 percent infection rate, according to the memo, but Hennepin County, which includes the city of Minneapolis, was at the time reporting a rate of 0.4 percent.

While Amazon has not said publicly how many employees have contracted the novel coronavirus disease, Bloomberg found the memo detailed “a sophisticated tracking regime” hidden from the public—unsurprising for Amazon, since it collects and uses mountains of data on everything it does.

Since March, front-line Amazon workers and contractors have complained that Amazon did not move quickly enough to stem the spread of disease in its facilities. The first Amazon warehouse employee known to have COVID-19 was diagnosed in March; one week later, cases were identified in at least nine warehouses.

Several Amazon employees, based both in warehouse locations and the company’s Seattle tech hub, were fired from their jobs

in April after speaking out about unsafe conditions in the fulfillment centers. In early June, a group of employees at the company's JFK8 warehouse in Staten Island filed a lawsuit alleging Amazon "relied on purposeful miscommunication with workers, sloppy contact tracing, and the culture of workplace fear it has instilled at JFK to ensure it can maintain productivity while reducing costs, even if that means workers come to work sick and cannot engage in proper hygiene, sanitizing, or social distancing while at work in order to stay healthy."

That has not abated, according to Recode, which yesterday published a report citing interviews with "dozens" of current and former employees. While those employees said safety conditions have improved in the warehouses since March, many added, "they have such limited work options that they keep showing up to sort, pack, and deliver shipments for Amazon even as they fear the company isn't doing enough to keep them safe during a global health crisis."

Amazon told Bloomberg in an emailed statement about the memo that "nothing is more important than the safety of our teams," adding, "We utilize a variety of data to closely monitor the safety of our buildings, and there is strong evidence that our employees are not proliferating the virus at work. What we see generally is that the overall rate of infection and increase or decrease of total cases is highly correlated to the overall community rate of infection."

The spokesperson did not provide an explanation for the infection rate inside MSP1, Bloomberg noted.

The MSP1 outbreak is Minnesota's 13th largest by case count, a state public health official told Bloomberg, saying that worse outbreaks were largely at meat-packing plants, which continue to face extreme challenges from COVID-19. Nor are the challenges confined to the US: Amazon was required to close all its warehouses in France temporarily in April, due to a

court ruling that it was failing to protect workers from COVID-19. Next door in Germany, Amazon workers went on strike yesterday in six locations. Union leader Orhan Akman said in a statement about the strike that “Amazon has so far shown no insight and is endangering the health of employees in favor of corporate profit,” according to CNBC.

https://arstechnica.com/?p=1688264

Detroit police chief cops to 96-percent facial recognition error rate

Enlarge / CCTV security guard in the mall building.

reader comments

50 with 35 posters participating

Share this story

Detroit’s police chief admitted on Monday that facial recognition technology used by the department misidentifies suspects about 96 percent of the time. It’s an eye-opening admission given that the Detroit Police Department is facing criticism for arresting a man based on a bogus match from facial recognition software.

Last week, the ACLU filed a complaint with the Detroit Police Department on behalf of Robert Williams, a Black man who was

wrongfully arrested for stealing five watches worth $3,800 from a luxury retail store. Investigators first identified Williams by doing a facial recognition search with software from a company called DataWorks Plus. Under police questioning, Williams pointed out that the grainy surveillance footage obtained by police didn't actually look like him. The police lacked other evidence tying Williams to the crime, so they begrudgingly let him go.

Now Vice's Jason Koebler reports that Detroit Police Chief James Craig acknowledged the flaws with its facial recognition software at a Monday event.

"If we would use the software only [to identify subjects], we would not solve the case 95-97 percent of the time," Craig said. "That's if we relied totally on the software, which would be against our current policy … If we were just to use the technology by itself, to identify someone, I would say 96 percent of the time it would misidentify."

As Craig notes, police officers in Detroit aren't supposed to arrest someone based solely on the results of a facial recognition search. And the Detroit police claimed that they didn't do that in the Williams case. A police spokeswoman told The New York Times that "the investigator reviewed video, interviewed witnesses, [and] conducted a photo lineup" before arresting Williams.

But this "investigation" was rather flimsy. The "photo lineup" consisted of showing photos to a security contractor who was not an eyewitness; he had only viewed the same surveillance footage police had used in the first place.

Research has found that the accuracy of facial recognition software varies by the race of the subject, with Black suspects being identified less often than white ones. And Koebler points out that the DPD's own statistics show the technology being used almost exclusively on Black suspects.

According to police data, 68 out of 70 facial recognition searches were done on Black suspects, while two had a race code of “U”—probably short for “unknown.”

The ACLU has called on the Detroit Police Department—and other police departments—to stop using facial recognition technology for investigations in light of its high error rate and racially disparate impact. Boston’s city council voted to ban the use of facial recognition technology last week.

https://arstechnica.com/?p=1688306

An embattled group of leakers picks up the WikiLeaks mantle

Getty Images

reader comments

20 with 14 posters participating

Share this story

For the past year, WikiLeaks founder Julian Assange has sat in a London jail awaiting extradition to the US. This week, the US Justice Department piled on yet more hacking conspiracy allegations against him, all related to his decade-plus at the helm of an organization that exposed reams of government and corporate secrets to the public. But in Assange’s absence, another group has picked up where WikiLeaks left off—and is also picking new fights.

For roughly the past year and a half, a small group of activists known as Distributed Denial of Secrets, or DDoSecrets, has quietly but steadily released a stream of hacked and leaked documents, from Russian oligarchs' emails to the stolen communications of Chilean military leaders to shell company databases. Late last week, the group unleashed its most high-profile leak yet: BlueLeaks, a 269-gigabyte collection of more than a million police filesprovided to DDoSecrets by a source aligned with the hacktivist group Anonymous, spanning emails, audio files, and interagency memos largely pulled from law enforcement "fusion centers," which serve as intelligence-sharing hubs. According to DDoSecrets, it represents the largest-ever release of hacked US police data. It may put DDoSecrets on the map as the heir to WikiLeaks' mission—or at least the one it adhered to in its earlier, more idealistic years—and the inheritor of its never-ending battles against critics and censors.

"Our role is to archive and publish leaked and hacked data of potential public interest," writes the group's cofounder, Emma Best, a longtime transparency activist, in a text message interview with WIRED. "We want to inspire people to come forward, and release accurate information regardless of its source."

Firefight time

In another message, Best sums up that mission in a Latin phrase that better captures the adversarial nature—and inherent controversy—of DDoSecrets' work: "*Veritatem cognoscere ruat cælum et pereat mundus*." Best translates the slogan to, "Know the truth, though the heavens may fall and the world burn."

For DDoSecrets, the firefight has already started. On Tuesday

evening, as media attention grew around the BlueLeaks release, Twitter banned the group's account, citing a policy that it doesn't allow the publication of hacked information. The company followed up with an even more drastic step, removing tweets that link to the DDoSecrets website, which maintains a searchable database of all of its leaks, and suspending some accounts retroactively for linking to the group's material.

Best says DDoSecrets, an organization with no address and whose shoestring budget runs mostly on donations, is still strategizing a response and the best workaround to publicize its leaks—potentially shifting to Telegram or Reddit—but has no intention of letting the ban halt its work. "'Too dangerous for Twitter' is some Nixonian shit I didn't expect," Best says.

From the start, DDoSecrets has distinguished itself by its willingness to publish not just the same sort of raw leaks and hacked files that WikiLeaks published for years, but also some that even WikiLeaks refused to. The group's first major release after its founding in late 2018 was a 175-gigabyte cache of Russian emails that included a collection of Russian political leaders' and oligarchs' communications, from the Russian interior ministry to arms exporter Rosoboronexport, provided by the Russian hacktivist group Sholtai Boltai along with other unknown sources.

WikiLeaks had obtained but declined to publish some of the same documents, *Foreign Policy* revealed in 2017, stating that it "rejects submissions that have already been published elsewhere or which are likely to be considered insignificant." But when DDoSecrets published the full Russian collection in early 2019, *The New York Times* covered the document dump as a kind of counterblow to the Kremlin's hacking and leaking operations that targeted the 2016 election.

Six months later, DDoSecrets returned with what it called #29 Leaks, a collection of 15 years of hacked emails from

Formations House, a London financial firm involved in the creation of shell companies. Those shell companies had been tied to allegations of money laundering, including by arms dealers, car smugglers, and the ousted Ukrainian president Viktor Yanukovych.

A few months after that, the pseudonymous hacktivist Phineas Fisher revealed that they had broken into the network of the Cayman National Bank and Trust, another player in the world of offshore banking. Fisher gave the resulting 2-terabyte trove of stolen data to DDoSecrets. The files revealed, among other things, how the former head of Azerbaijan's national security agency allegedly used embezzled funds to buy UK properties. DDoSecrets' Best says that journalists are still digging into the massive data set today.

With BlueLeaks, however, DDoSecrets has, for the first time, published a major leak of files from US organizations, raising the stakes. Activists and journalists combing through the files immediately found evidence that the FBI had monitored the social accounts of protesters on behalf of local law enforcement and tracked bitcoin donations to protest groups. The leak also includes personally identifiable information about police officers and even banking details—though Best says BlueLeaks tried to redact all identifiable victim information—which has fueled controversy around the publication and no doubt contributed to the group's Twitter ban. (Twitter did not respond to a request for comment.) "The public has an interest in the identities of public servants," Best writes.

That red-hot disclosure, perfectly timed to follow the global protests in the wake of police killing of George Floyd, shows how the organization is coming into its own, says Birgitta Jonsdottir, a former member of WikiLeaks and the Icelandic parliament who now serves as an adviser to DDoSecrets. "They remind me of the people who were risking a lot for WikiLeaks back in the day," Jonsdottir says. "There's been a vacuum for

a long time. So I'm just glad this is taking off, with this very important leak at this time."

Learning from the experience of others

But Best, who identifies with the pronouns they/them, says that DDoSecrets has learned from WikiLeaks' mistakes as well as its successes. Best has collaborated with WikiLeaks in the past—the relationship was complicated; Best later published a trove of the group's own leaked chats in 2018—and points to a long list of what they see as WikiLeaks' missteps: publishing materials without a source's permission, as they found to be the case of the leak of emails from the Turkish government's ruling party; inexplicably declining to publish leaked files, as with the Russia dump that DDoSecrets later published; or adding unnecessary editorial spin to documents, as they argue WikiLeaks did with the Vault7 leak of CIA secrets.

Best also faults Assange specifically for trying to hide the fact that certain documents are provided by state-sponsored hackers, as when he intimated that the documents taken from the Democratic National Committee and the Clinton Campaign might have come from murdered Clinton staffer Seth Rich. In fact, Russian military intelligence hackers stole the documents and provided them to WikiLeaks. DDoSecrets, Best says, won't shy away from publishing files stolen by state-sponsored hackers if they're of real public interest. But those documents will be clearly labeled as coming from state-sponsored hackers when DDoSecrets can determine as much, they say, and will be kept on a portion of the site devoted to the spoils of government hacking. "Valid information is valid regardless of the source," Best says. "But the source is important context."

DDoSecrets is also taking a very different tack from WikiLeaks in protecting the anonymity of sources. It doesn't host a

WikiLeaks-style submission system on a server protected by the anonymity software Tor, as WikiLeaks and most other leaking sites have done. Best says they don't actually believe that DDoSecrets, an organization without a physical presence or a headquarters, could sufficiently protect a physical server running an anonymous submission system such as SecureDrop. Instead, the group simply provides a list of security tool recommendations to sources like Tor and the anonymous, ephemeral operating system Tails, as well as a variety of means to reach them via an encrypted message.

The approach hints that the group sees principled hackers as its core sources rather than non-technical leakers or whistleblowers inside of companies, says Gabriella Coleman, a hacker-focused anthropologist at McGill University who wrote a seminal book on the hacktivist group Anonymous and is friendly with some of DDoSecrets' staff. The group's name, a reference to the cybersecurity term "distributed denial of service," and its relationship with Phineas Fisher further suggests an intended audience of hackers. "Using a name like that, it's signaling a certain message to the hacker and hacktivist world, where they have certain relationships," says Coleman. "They're happy to accept leaks from whistleblowers, but they come from the hacker world. They're going to be very well positioned to take leaks from more progressive hackers." (Best declined to comment on the group's sources, or what fraction are insider leakers versus outside hackers.)

Perhaps most importantly, Best says DDoSecrets wants to avoid the cult of personality that formed around Julian Assange. The WikiLeaks leader had exerted near-monarchic rule before being indicted for computer hacking conspiracy and arrested in London's Ecuadorian embassy, where he had sought asylum, last spring. Best says DDoSecrets is moving toward a "co-op" model with a "horizontal structure" of leadership, with no single person in charge of the group's direction.

Former WikiLeaker Jonsdottir, who has both criticized Assange

and called for support for him after his arrest, believes this time will be different. “I don’t see anyone in the organization that can be made into the stories we had about Assange, a mysterious superhero,” Jonsdottir says. “Like Tina Turner said, we don’t need another hero.”

The Twitter ban following its BlueLeaks publication represents a setback for the group. But Jonsdottir says it also shows the importance of the work they’re doing. “They will definitely rise above this,” Jonsdottir says. “Somebody trusted them with a massive leak at a critical time. And I’m excited to see if it will help spawn more like it.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1687754

FCC helps Charter avoid broadband competition

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

reader comments

61 with 41 posters participating

Share this story

The Federal Communications Commission is helping Charter avoid broadband competition in New York State with a decision that

will block government funding for other ISPs in locations where Charter is required to build.

The FCC plans to award ISPs up to $16 billion over 10 years from the Rural Digital Opportunity Fund (RDOF) in a reverse auction scheduled to begin in October. The FCC said in an announcement yesterday that it "granted Charter Communications' waiver request to exclude 2,127 census blocks in New York from the eligible areas list because the company will deploy broadband in those locations pursuant to a settlement reached with the State of New York."

Separately, the FCC denied a Frontier Communications request to exclude nearly 17,000 census blocks in parts of 29 states from the auction.

RDOF rules block funding in census blocks that already have home-Internet access at speeds of at least 25Mbps downstream and 3Mbps upstream. RDOF rules also block funding in census blocks where at least one ISP has been awarded money from any federal or state broadband-subsidy program "to provide 25/3Mbps or better service." But as we previously reported, that rule would not prevent ISPs from getting funding to serve parts of New York where Charter is required by a merger condition to offer service but in which it hasn't yet finished construction. Charter petitioned the FCC for a waiver to ban RDOF funding in those census blocks "in which Charter has unfunded but nonetheless binding state obligations to deploy at least 25/3Mbps broadband service."

Charter's New York project is required by conditions the state government imposed on its purchase of Time Warner Cable. Charter failed to meet interim deadlines in that project but got an extra year to comply in a settlement in which it agreed to pay $12 million toward other new broadband deployments. Under the new, postponed deadline, Charter is required to finish deploying service to 145,000 homes and businesses in Upstate New York by September 30, 2021. Charter offers service

under the Spectrum brand name.

The FCC said excluding the New York census blocks from this year's auction "will further the Commission's goal that Rural Digital Opportunity Fund support flow to areas that are in the most need of universal service support to advance broadband deployment—those that remain wholly unserved with broadband speeds of 25/3Mbps."

The FCC originally shut all of New York out of the auction, but it reversed that decision after protest. Under yesterday's decision, 47,024 homes and businesses in New York are eligible for funding from this year's auction.

There are about 11 million census blocks in the US, but several million are unoccupied. The size of each census block varies from "a block in a city bounded on all sides by streets" to "hundreds of square miles" in remote areas, the Census Bureau says.

FCC denies Frontier

In another portion of the same order, the FCC yesterday said it will allow funding in 16,987 census blocks where Frontier claimed it offers 25/3Mbps service. Frontier, which filed for bankruptcy in April 2020, drew skepticism when it claimed to the FCC that it had deployed 25/3Mbps broadband to those 16,987 census blocks since June 2019. Frontier later "explained that its list of 16,987 census blocks does not reflect new builds since June 2019, but rather more accurate reporting on the fastest speeds that are available in certain blocks," the FCC said.

The FCC agreed there is reason for skepticism. "Given the numerous and significant concerns in the record regarding the validity of Frontier's filing, including its own admission that it had misfiled its June 2019 data, errors in its challenge that it sought to revise, and inconsistent

explanations for its challenge, the commission denied Frontier's challenge," the FCC said.

Frontier urged the FCC to exclude the 16,987 census blocks in a filing on April 10. But Frontier gave up on that request a month and a half later, telling the FCC on May 23 that it "would welcome the inclusion into the RDOF auction the challenged census blocks where Frontier provides service at speeds of 25/3Mbps and greater." These census blocks are in 29 states; since the original filing, Frontier completed a sale of its operations in four of those states.

Nationwide, the FCC said it determined that 5,392,530 homes and businesses count as "unserved locations" where this year's $16 billion auction can distribute funding. The RDOF's overall budget is $20.4 billion over 10 years. The remaining $4.4 billion will be distributed after the FCC collects more accurate broadband-mapping data.

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

https://arstechnica.com/?p=1687664

Chinese bank requires foreign firm to install app with covert backdoor

reader comments

32 with 21 posters participating

Share this story

A large, multinational technology company got a nasty surprise recently as it was expanding its operations to China. The software a local bank required the company to install so it could pay local taxes contained an advanced backdoor.

The cautionary tale, detailed in a report published Thursday, said the software package, called Intelligent Tax and produced by Beijing-based Aisino Corporation, worked as advertised. Behind the scenes, it also installed a separate program that covertly allowed its creators to remotely execute commands or software of their choice on the infected computer. It was also digitally signed by a Windows trusted certificate.

Researchers from Trustwave, the security firm that made the discovery, have dubbed the backdoor GoldenSpy. With system-level privileges to a Windows computer, it connected to a control server located at ningzhidata[.]com, a domain Trustwave researchers said is known to host other variations of the malware. The backdoor included a variety of advanced features designed to gain deep, covert, and persistent access to infected computers.

According to Thursday's post, those features include:

> - *GoldenSpy installs two identical versions of itself, both as persistent autostart services. If either stops running, it will respawn its counterpart. Furthermore, it utilizes an exe protector module that monitors for the deletion of either iteration of itself. If deleted, it will download and execute a new version. Effectively, this triple-layer protection makes it exceedingly difficult to remove this file from an*

infected system.

- *The Intelligent Tax software's uninstall feature will not uninstall GoldenSpy. It leaves GoldenSpy running as an open backdoor into the environment, even after the tax software is fully removed.*
- *GoldenSpy is not downloaded and installed until a full two hours after the tax software installation process is completed. When it finally downloads and installs, it does so silently, with no notification on the system. This long delay is highly unusual and a method to hide from the victim's notice.*
- *GoldenSpy does not contact the tax software's network infrastructure (i-xinnuo[.]com), rather it reaches out to ningzhidata[.]com, a domain known to host other variations of GoldenSpy malware. After the first three attempts to contact its command and control server, it randomizes beacon times. This is a known method to avoid network security technologies designed to identify beaconing malware.*
- *GoldenSpy operates with SYSTEM level privileges, making it highly dangerous and capable of executing any software on the system. This includes additional malware or Windows administrative tools to conduct reconnaissance, create new users, escalate privileges, etc.*

Thursday's post said that Trustwave threat analysts identified "similar activity" at a second company but don't have many other details. The security firm has found variations of GoldenSpy that date back to late 2016, but the first indication the backdoor was actually used in the wild is in April, when the campaign against the tech company began. Researchers still don't know the scope, purpose, or actors behind the threat. Trustwave didn't identify the two companies that encountered GoldenSpy or the local Chinese bank that required that Intelligent Tax be installed. Representatives of

Aisino Corporation didn’t immediately respond to an email seeking comment for this post.

https://arstechnica.com/?p=1687527

Three cops fired after accidental dashcam activation captures racist rants



Enlarge / Members of the Wilmington, North Carolina, police force taking part in the city’s annual Azalea Festival parade in April 2019.

reader comments

222 with 123 posters participating

Share this story

Three North Carolina police officers were fired from their jobs this week after investigators found incredibly racist, troubling conversations, and threats of violence accidentally recorded by the cops' own dashboard camera.

The dashboard camera in Officer Kevin Piner's patrol car captured more than 46 minutes of relevant footage from a two-hour recording, Wilmington Police Chief Donny Williams said Wednesday.

According to the department's report (PDF), Piner's camera was recording due to "accidental activation." That activation ended up capturing Piner and two other officers, Jessie Moore and Brian Gilmore—all white—discussing Black members of the force as well as local protesters, using well-known racist slurs. At one point, Moore said a local magistrate, a Black woman, "needed a bullet in her head," before the three discussed their feelings that a civil war was coming, for which all three claimed to be ready. "We are just gonna go out and start slaughtering them fucking n——s," Piner added.

The conversations "were brutally offensive and deserved immediate action," Williams said. "When I first learned of these conversations, I was shocked, saddened, and disgusted. There is no place for this behavior in our agency or our city and it will not be tolerated."

Williams also added that he was petitioning the court to determine whether the footage could be released publicly, in accordance with North Carolina law.

Proof vs. accountability

Police body or dashboard-mounted cameras are often promoted as a boon to police accountability, and the Wilmington case seems to prove why.

Many state and local governments have rushed to adopt resolutions in recent weeks calling for increased camera usage or funding, in response the ongoing nationwide protest movement against police brutality and in support of Black communities. In New York state, for example, the state Assembly just passed legislation requiring body cameras for all state police. Speaker Carl Heastie said about the measure, "As one of the largest state police agencies in the country, the New York State Police should be one of the first agencies to set an example, to show others how to properly use body cams to deliver transparency and accountability to the public."

Sometimes the footage does indeed work as intended. In 2017, for example, 34 criminal cases were thrown out in Maryland after footage from body-worn cameras showed police planting drugs near suspects.

But the technology is not in and of itself a panacea. "Police departments large and small are rolling out expensive body-camera programs without consistent answers to the questions or, according to policy experts, convincing evidence that the cameras ensure the level of accountability that the public demands," The New York Times reported back in 2017, and those questions do not yet seem to have answers.

A study conducted in Washington, DC, in 2017 found no change in police behavior or citizen complaints after police in the nation's capital began wearing body cameras. In 2019, researchers who published a meta-analysis of 70 studies on police body-worn cameras found that DC was not alone, and cameras did not have "a consistent or significant effect" on officer behavior or complaints overall.

Privacy

Privacy advocates have also warned consistently about the dangers posed by body-worn police cameras, not only when

police are speaking with individuals who deserve privacy, but also in situations such as mass protests when demonstrators believe they have anonymity.

“Reform activists should not simply demand hardware,” the American Civil Liberties Union wrote in a blog post today. “They should demand effective body camera *programs*, which include not just cameras but also strong policies and institutional practices to make those cameras effective.”

https://arstechnica.com/?p=1687433

Graham, Cotton introduce yet another attempt to torpedo encryption



Enlarge / This dog was part of widespread protests against the FBI's attempts to penetrate iPhone encryption.

reader comments

132 with 96 posters participating, including story author

Share this story

On Tuesday, Sens. Lindsey Graham (R-S.C.), Tom Cotton (R-Ark.), and Marsha Blackburn (R-Tenn.) introduced yet another bill attempting to poke holes in data encryption, called the Lawful Access To Encrypted Data Act. This bill follows previous US efforts to weaken encryption, including March's proposed EARN IT Act and demands made by US Attorney General William Barr in his 2019 keynote address at the International Conference on Cyber Security.

A press release from the Senate Judiciary Committee—which is chaired by Graham—describes the bill as "a balanced solution

that keeps in mind the constitutional rights afforded to all Americans, while providing law enforcement the tools needed to protect the public from everyday violent crime and threats to our national security." It goes on to emphasize—in both bold and italic text—that the bill would "only" require service providers to grant law enforcement a back door after a court issues a warrant.

Graham expresses his personal position in strong terms:

> *Terrorists and criminals routinely use technology, whether smartphones, apps, or other means, to coordinate and communicate […] tech companies have refused to honor [court orders] and assist law enforcement in their investigations. My position is clear: After law enforcement obtains the necessary court authorizations, they should be able to retrieve information to assist in their investigations. Our legislation respects and protects the privacy rights of law-abiding Americans.*

Unfortunately, as is typical for these resolutions, Graham's expressed ideas don't adhere to technological reality. In order for a service provider to "honor and assist" law enforcement investigations in the way Graham demands, it would necessarily—and fatally—have to compromise the very encryption it offered in the first place. This would apply to every consumer the provider services (American or otherwise), whether a warrant were issued or not.

Encryption doesn't work that way

Providing the sort of backdoor Graham and company keep asking for means, among other things, providing the service provider itself access to "encrypted" data. This, in turn, opens that provider's customers up to privacy violations from the service provider—or rogue employees of the service provider—themselves, which in turn would break much of the

security model of modern cloud services. This would gravely impact not only end consumer privacy but enterprise business security as well.

In recent years, large cloud providers such as Amazon, Microsoft, and Google have made big and successful pushes to convince large businesses to host increasingly confidential business data in their data centers. This is only feasible because of secure encryption using keys inaccessible to the cloud provider itself. Without provider-opaque encryption, those businesses would return to storing critically confidential data only in self-managed and controlled private data centers—increasing cost and decreasing scalability for those businesses.

This, of course, only scratches the surface of the true impact of such a misguided effort. Secure encryption is an already widely available technology, and it doesn't require massive infrastructure to implement. There is no reason to assume that the very terrorists Graham, Cotton, and Blackburn invoke wouldn't simply revert to privately managed software without holes poked in it were such a bill to pass.

There's also no reason to assume that the service providers themselves would be the only ones able to access the critical loopholes LAEDA would require. It's difficult to imagine that such vulnerabilities would not rapidly become widely known and be exploited by garden-variety criminals, foreign and domestic business espionage units, and foreign nations.

Follow-on economic impact

Finally, the passage of a US bill such as LAEDA would not constrain service providers in foreign countries. Another likely impact of such a bill would be to simply shift such services offshore to European and Asian providers—reducing American tax revenues and technical prominence, while pushing the very data Graham so badly wants access to even further out

of his reach.

Deputy Director Evan Greer of advocacy group Fight for the Future gave Ars the following statement about LAEDA and a similar predecessor, the EARN IT Act:

> *Politicians who don't understand how technology works need to stop introducing legislation like this. It's embarrassing at this point. Encryption protects our hospitals, airports, and the water treatment facilities our children drink from. Security experts have warned over and over again that weakening encryption or installing back doors will make everyone less safe, not more safe. Full stop. Lawmakers need to reject the Lawful Access to Encrypted Data act along with the EARN IT act. These bills would enable mass government surveillance while doing nothing to make children, or anyone else, any safer.*

Although the actual text of the bill does not seem to be publicly available yet, the Judiciary Committee's press release outlines a few key points. The attorney general would be prohibited from issuing directives with specific technical steps for complying with the act—but would be allowed to issue directives requiring compliance. The AG would also be empowered to direct service providers or device manufacturers to report both their ability to comply and timeline for implementation of the loopholes necessary to comply.

The bill specifies that service providers and device manufacturers issued such directives would be compensated with government funding for reasonable costs incurred in compliance with that directive. It also establishes a prize competition to award participants who "create a lawful access solution in an encrypted environment, while maximizing privacy and security."

https://arstechnica.com/?p=1686929

Twitter terminates DDoSecrets, falsely claims it may infect visitors



Aurich Lawson / Getty

reader comments

58 with 42 posters participating, including story author

Share this story

Four days after leak publisher DDoSecrets circulated private documents from more than 200 law enforcement agencies across the United States, Twitter has permanently suspended its account and falsely claimed that the site may infect users with malware.

“Your account, DDoSecrets, has been suspended for violating

the Twitter rules," this email, which Twitter sent to the account holders, said. The message cited rules against "distribution of hacked material" and went on to say:

> *We don't permit the use of our services to directly distribute content obtained through hacking that contains private information, may put people in physical harm or danger, or contains trade secrets.*
>
> *Note that if you attempt to evade a permanent suspension by creating new accounts, we will suspend your new accounts. If you wish to appeal this suspension, please contact our support team.*

BlueLeaks asks: Why us and not WikiLeaks?

DDoSecrets describes itself as a "transparency collective, aimed at enabling the free transmission of data in the public interest." On Friday, it published BlueLeaks, a 269-gigabyte trove of documents that KrebsOnSecurity reported was obtained through the hack of a Web development company that hosted documents on behalf of police departments. Some of the documents exposed police candidly discussing responses to demonstrations protesting what a Minnesota district attorney has charged was the murder of George Floyd, a Black man who died while handcuffed as a Minneapolis Police Department officer pressed a knee on his neck for nearly nine minutes. As of Tuesday, Derek Chauvin, who has since been fired, had not entered a plea.

A Twitter spokesperson confirmed that the company had permanently suspended the DDoSecrets account for violating the social media site's rules barring hacked materials. The spokesperson said the material (1) contained unredacted information that could put people at risk of real-world harm

and (2) ran afoul of a policy that forbids the distribution of material that is obtained through technical breaches and hacks, as publishers of DDoSecrets claimed had been done.

DDoSecrets co-founder Emma Best criticized the suspension and noted that the Twitter account for WikiLeaks remains active despite its publishing vast troves of private information resulting from the 2016 hack of the Democratic National Committee and members of the Hillary Clinton campaign. WikiLeaks has also tweeted links to its Vault 7 series, which published details about closely guarded CIA hacking programs.

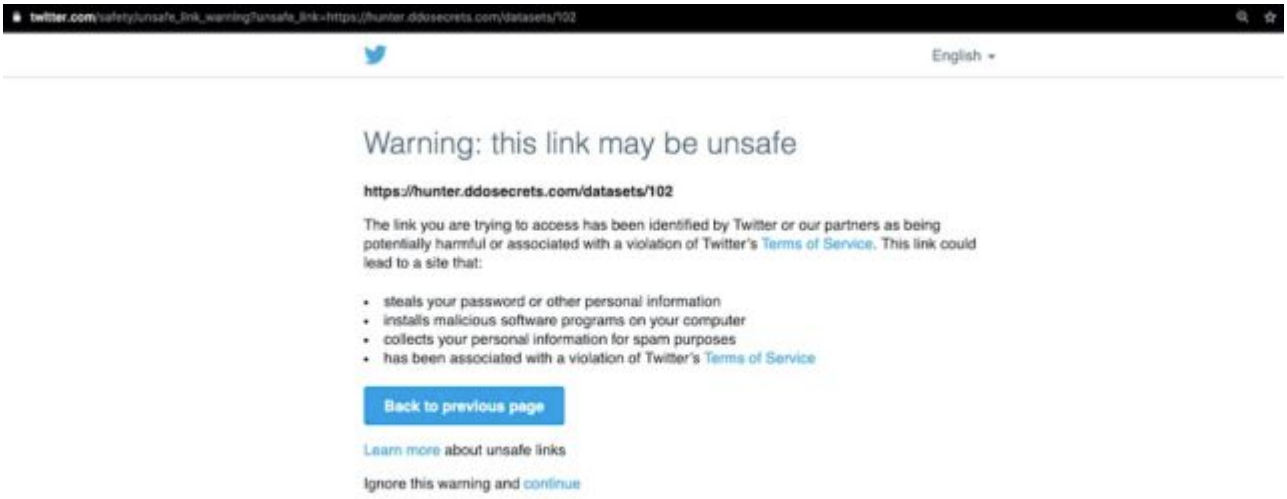
Other accounts associated with the Anonymous hacking movement have also escaped suspensions. Twitter was also slow to suspend from Guccifer 2.0 and the Dark Overlord, the monikers of two purported hackers, both of whom also published extensive amounts of personal information obtained through hacking and tweeted the links.

“@DDoSecrets has worked with dozens of major news outlets across the world and published terabytes of data uncovering money laundering schemes, corruption, and more,” Best tweated. “Now we’re being censored for publishing the #BlueLeaks files about law enforcement.”

> *.@DDoSecrets has worked with dozens of major news outlets across the world and published terabytes of data uncovering money laundering schemes, corruption, and more.*
>
> *Now we’re being censored for publishing the #BlueLeaks files about law enforcement https://t.co/MBKQ7JRW6A*
>
> *— Emma Best  (Mx. Yzptlk) (@NatSecGeek) June 23, 2020*

Fearmongering

Twitter users who clicked on tweeted links to the DDoSecrets.com site received a message from Twitter warning, with no evidence, that the site may install malware, steal passwords or other sensitive data, or collect personal data for purposes of sending spam.



This security check from Web security firm Sucuri found no malware on the site, although the firm did note that it was blocked by fellow security firm McAfee.

Best said the only malware on the site are binary samples of malware such as the Stuxnet worm that infected Iran about a decade ago and attachments found in emails posted to the site. Best said that DDoSecrets critics have been falsely reporting to security firms that the site is malicious in an attempt to make the site unavailable to users of antivirus products.

The Twitter spokesperson didn’t answer questions about the basis for the claims. The spokesperson also didn’t say what distinguished materials published by DDoSecrets from those published by WikiLeaks. McAfee representatives weren’t immediately available for comment.

Best told Wired that prior to publishing BlueLeaks, DDoSecrets

spent a week scrubbing about 50 gigabytes of material disclosing sensitive details about crime victims, children, unrelated private businesses, health care companies, and retired veterans' associations. The co-founder conceded, however, that the team "probably missed things."

Critics have increasingly complained that Twitter's rules for removing tweets and accounts it deems abusive or harmful are inconsistent. The social media site's permanent suspension of DDoSecrets and its unsubstantiated warnings the site may engage in malicious behavior is only going to further those charges.

https://arstechnica.com/?p=1686803

Google, Amazon condemn Trump order cutting off foreign worker visas



Enlarge / Illustration of a green card sitting on an open passport. Green card holders are not currently affected by the new order, but the administration says immigration-restricting order will leave 525,000 jobs vacant this year for US citizens to fill.

reader comments

186 with 103 posters participating

Share this story

Tech firms are pushing back against the Trump administration after President Donald Trump yesterday issued an order suspending the issuance of a wide range of work visas, including the type that allows high-skilled workers and their families to enter the country and work for American technology companies.

Monday’s proclamation renews and expands on an earlier order issued in April.

Both the April and June orders claim that admitting workers from other nations at this time would put the United States at an economic disadvantage while the nation tries to recover from massive job losses related to COVID-19. The new order extends the existing limitations on immigration into the US through at least the end of the year, and it additionally prohibits several categories of non-immigrant worker visas from being issued in the back half of 2020. The visas now being limited include types H-1B, which applies to high-skilled degree-holding workers; H-2B, which applies to temporary workers in non-agricultural industries; J, which applies to exchange visitors, both educational and professional; and L, which applies to individuals transferring to a US location within the company for which they already work.

The order does not apply to anyone who already holds a green card, who is the spouse or child of a US citizen, or whose entry "would be in the national interest" as determined by the State Department or the Department of Homeland Security, including health care workers involved in COVID-19 research or treatment. Agricultural workers entering the country temporarily are also exempt. The order applies only to new visas and does not affect those who already have been approved for a relevant visa or are already in the US.

Big Tech is Big Mad

The H1-B program is capped at 85,000 visas per year, and large US tech firms compete mightily to hire foreign workers through that program. Google alone filed for more than 7,600 H-1B visas in fiscal year 2019, according to federal data compiled by recruiting firm Dice.

"Immigrants have not only fueled technological breakthroughs and created new businesses and jobs but have also enriched American life," a Google spokesperson said in response to the

new executive order. “America’s continued success depends on companies having access to the best talent from around the world. Particularly now, we need that talent to help contribute to America’s economic recovery.”

Tech rivals Facebook and Amazon also echoed the sentiment that choking off the pipeline for international talent would hinder, rather than help, US economic recovery. “The move to keep highly-skilled talent out of the US will make our country’s recovery even more difficult,” Facebook said. “Highly-skilled visa holders play a critical role in driving innovation—at Facebook and at organizations across the country—and that’s something we should encourage, not restrict.”

“We oppose the Administration’s short-sighted action,” Amazon said bluntly. “The value of high-skilled visa programs is clear, and we are grateful for the many Amazon employees from around the world that have come to the US to innovate new products and services for our customers.”

Major tech-industry trade groups, including the Internet Association and the Information Technology Industry Council, also denounced the administration’s move.

Although major US firms all employ workers on H-1B guest worker visas, the program has not been without controversy. A February report from OneZero found that many employees working for US firms on H-1B visas experience additional pressure, discrimination, or fear at work due to their immigration status. “I believe that H-1B employees tend to tolerate more bullshit from managers because they cannot move to another company that easily, and they cannot just rage-quit,” one employee told OneZero.

https://arstechnica.com/?p=1686565

If T-Mobile’s giant outage affected you, now’s your chance to tell the FCC



Enlarge / A pigeon rests on a T-Mobile logo outside a mobile phone store, operated by Deutsche Telekom AG, in Munich, Germany, on Monday, Feb. 6, 2017.
Getty Images | Bloomberg

reader comments

41 with 33 posters participating, including story author

Share this story

The Federal Communications Commission is kicking off its

investigation of last week's T-Mobile outage by seeking public comment. Government agencies, public safety entities, businesses, and individuals are encouraged to submit comments about their experiences during the 13-hour outage.

"We seek comment on the impact of these outages from the perspective of affected public safety entities, as well as state and local governments," the FCC said in a public notice today. "Are there estimates of how many calls, including 911 calls, failed or otherwise affected by the outage? What was the effect of the outage on public safety activities and government services across the country? Was there a disruption of data services relied on by public safety entities and state and local governments?"

The outage "prevented customers from making calls, receiving calls, and in some cases, sending text messages over T-Mobile's Voice-over LTE (VoLTE) network," and social media reports indicated that 911 calling was affected, the FCC notice said. Besides government and public safety organizations, the FCC is seeking comment on "this outage's impact from the perspective of affected individual and enterprise consumers."

The public notice asks these questions of businesses and individuals:

> *How did consumers learn about the outage? Was T-Mobile's communication about the outage appropriate, timely, and effective? Were consumers of T-Mobile's network able to successfully make or receive all calls, some calls, or no calls at all? Were consumers of other communications service providers able to successfully complete calls to consumers of T-Mobile's network? Were consumers' text messages successfully sent or received during the outage? Did consumers on T-Mobile's network experience a disruption of data services during the outage? Were consumers able to use alternative measures, such as "FaceTime, iMessage, Google*

> *Meet, Google Duo, Zoom, Skype and others to connect" during the outage, and was that method of communication successful and effective? What effect did the outage have on businesses and providers of critical services, such as hospitals? What effect did the outage have on consumers' personal activities?*

The FCC set a deadline of July 8 for submitting comments. The docket where comments can be filed online is available here. Read the public notice for instructions on how to submit comments by mail.

FCC Chairman Ajit Pai called the outage "unacceptable" and said the FCC will be "demanding answers," as we reported last week. That doesn't mean T-Mobile will face any punishment. In a previous case, Pai called mobile carriers' response to Hurricane Michael in Florida "completely unacceptable," but imposed no punishment.

T-Mobile's explanation of last week's network failure said "the trigger event is known to be a leased fiber circuit failure from a third-party provider in the Southeast." Mobile networks are designed to survive such failures, but in this case T-Mobile said its network "redundancy failed us and resulted in an overload situation that was then compounded by other factors." The overload then caused an "IP traffic storm that spread from the Southeast to create significant capacity issues across the IMS (IP multimedia Subsystem) core network that supports VoLTE calls." To prevent recurrences, T-Mobile said it has "worked with our IMS and IP vendors to add permanent additional safeguards to prevent this from happening again and we're continuing to work on determining the cause of the initial overload failure."

https://arstechnica.com/?p=1686657