Feds decline to release list of 147 nursing homes stricken by coronavirus

Enlarge / Elder Hands

reader comments

90 with 58 posters participating, including story author

Share this story

Two federal agencies, the Centers for Disease Control (CDC) and the Centers for Medicare and Medicaid Services (CMS), have a list of 147 nursing homes where at least one resident has contracted COVID-19. But The Washington Post reports that the agencies are refusing to release this list to the public.

“According to CDC data shared with CMS, 147 nursing homes across 27 states have at least one resident with COVID-19,” the CMS wrote in the sixth paragraph of a Monday press release about increased nursing home inspections. But when the Post asked the CMS for the list, the agency referred the paper to the CDC. A CDC spokesman told the Post that he was “not sure” the list would be “released at this time.”

“It’s terrible—people have a right to know where this is happening,” nursing professor Charlene Harrington told the paper. “These nursing homes should be made public so that people have the option to take people out.”

Nursing homes are a particular concern during the COVID-19 pandemic because elderly people are at much higher risk of dying from the coronavirus. It’s difficult to quarantine

residents in nursing homes because most have staff that care for patients and then return home.

Some nursing homes have publicly announced when residents or staff contract COVID-19. A public announcement allows anyone who lives, works, or visits the facility to take added precautions. It’s not clear how many of the 147 facilities on the CDC list have been disclosed publicly.

The Post notes that Florida officials have also come under pressure to release a list of 19 Florida nursing homes with COVID-19 outbreaks. Florida officials have declined to provide the list, citing privacy laws.

https://arstechnica.com/?p=1663191

---

737 Max fix slips to summer—and that’s just one of Boeing’s problems

Enlarge / The 737 Max is just the most high-profile of Boeing’s crises.

reader comments

64 with 51 posters participating, including story author

Share this story

The past 10 months have not been good for Boeing for all sorts

of reasons—capped off by the failure of the company's Starliner commercial crew vehicle to achieve the right orbit in its uncrewed premier in December. But the biggest of the company's problems remains the 737 Max, grounded since last spring after two crashes that killed 346 people between them. Combined, the crashes are the worst air disaster since September 11, 2001.

Both were at least partially caused by a sensor failure with no redundancy and a problem with MCAS (the new software controlling the handling of the aircraft) that the air crews had not been trained to overcome.

Boeing executives are now telling the company's 737 Max customers that the software fix required to make the airliner airworthy will not be approved in the near future, and that it will likely be June or July before the Federal Aviation Administration certifies the aircraft for flight again—meaning that the aircraft will have been grounded for at least 16 months.

The FAA, for its part, has not committed to any timeframe for re-certifying the aircraft. In an emailed statement, an FAA spokesperson said, "We continue to work with other safety regulators to review Boeing's work as the company conducts the required safety assessments and addresses all issues that arise during testing."

In the past, Boeing could rely on its space and defense divisions to keep the company rallying when its commercial airliner business faltered, and vice versa. But over the past decade, Boeing's defense, space, and security businesses—consolidated into a single division in 2017—have not been booming. And growth in overall revenues came largely because of the sales of the 737 Max.

Boeing, once known for a culture of safety and rigorous engineering, has over the past decade gained a reputation for

sloppy work, blown deadlines, and flat-out scandal.

Space cases

Enlarge / The crew module of Boeing’s CST-100 Starliner spacecraft is lifted onto its service module on October 16 inside the Commercial Crew and Cargo Processing Facility at Kennedy Space Center in Florida.
The CST-100 Starliner commercial crew spacecraft was supposed to be a slam dunk for Boeing—a contest that, with the company’s reputation in space systems (as a partner in United Launch Alliance, and one of the major contributors in building and sustaining the International Space Station), would have seemed to have been its to lose.

Boeing has been doing just that. The program suffered a series of setbacks, including a problem with a pad test of its abort system. In November, NASA’s inspector general reported that the Starliner would cost 60 percent more per seat than SpaceX’s Crew Dragon. The Crew Dragon completed a successful unmanned demo in March of last year. And despite an explosive

failure on the launch pad last April, SpaceX managed to come back and complete its last unmanned test this month.

The failure to reach the ISS's orbit with the Demo 1 launch of the Starliner was a very expensive software failure. And while the rest of the flight was proclaimed to be successful—including a soft landing on land at White Sands Space Harbor in New Mexico—there were other problems related to the failure of thrusters on the service module connected to the way they were used to try to raise Starliner's orbit. Those thruster issues may have caused the spacecraft to fail other tests.

Meanwhile, Boeing's piece of the Space Launch System has had a long road toward delivery, with its first core stage just completed. The delays have further pushed back all of the programs linked to it, including NASA's current lunar plans, and the rocket is unlikely to see its first flight until 2021.

Sure, most of the spending on the program—72 percent—has been on overhead costs. So not all of the cost overruns are Boeing's fault. But Boeing's costs in the cost-plus program have been growing unexpectedly. All that apparently doesn't matter to NASA, which is going ahead and buying the rockets—offering up $270 million on top of the cost-plus contract to deliver 10 of them.

Tanking it

Enlarge / Boeing’s KC-46 aerial refueling tanker conducts receiver-compatibility tests with a US Air Force C-17 Globemaster III from Joint Base Lewis-McChord in 2016.
US Air Force

Boeing’s KC-46 Pegasus tanker program has the shadow of scandal hanging over it. Why? Because it forced Boeing’s CEO-before-last to resign, and it put the company’s chief financial officer (and former Air Force procurement officer) in jail. But because the competition was a Northrop partnership with Airbus, Boeing still managed, somehow, to swing enough political clout to get the contract anyway. And the company has run into delays and difficulties ever since.

The program is $3 billion over budget and three years behind schedule. Debris left behind from manufacturing the airframes has slowed down delivery of the planes. There are problems with the system used to steer the refueling boom, and it looks like the aircraft won’t be able to use wing-mounted refueling pods until at least the middle of this year—limiting the tanker’s aerial refueling role. And that is its main job.

Boeing took a $272 million hit on the program because the company had to redesign the tanker's wiring. Then there were "technical and supply chain" problems that further delayed the program in 2016.

While the Air Force has begun taking delivery on the tankers, the aircraft entered initial operational capability testing two years behind schedule. And last year, the aircraft was banned from carrying passengers or cargo—a big part of its mission—after cargo broke free of lockdowns during flight.

To top it off, delivery is behind schedule, and the Air Force doesn't expect to reach its full operational capability with the aircraft until 2022, maybe. As of the end of the 2019 fiscal year, the Air Force had seen delivery of 18 aircraft to air bases, with one more completed and awaiting delivery—making the total quantity one greater than what Boeing was supposed to deliver in 2017 under the contract.

A new legacy

Boeing has a bunch of other military programs in play. But with the F/A-18 Super Hornet now entering a legacy phase with the Navy, Marine Corps, and fewer buyers overseas, and with Boeing taking a backseat in a partnership with Lockheed's Sikorsky for Army helicopter competitions, the company's military footprint could be shrinking fast. A lot is riding, literally, on Boeing's space operations going forward.

But given the problems Boeing's programs have faced over the past few years, capped off by the 737 Max MCAS disaster, we shouldn't wonder that Congress is taking an interest in getting more oversight over the company. And the future of all Boeing's businesses is riding on the company regaining trust.

https://arstechnica.com/?p=1646983

Brazil prosecutes Glenn Greenwald in “attack on press freedom”

Enlarge / Glenn Greenwald speaks during a hearing at the Lower House’s Human Rights Commission in Brasilia, Brazil, on June 25, 2019.

reader comments

71 with 48 posters participating

Share this story

Brazilian prosecutors today charged journalist Glenn Greenwald with cybercrimes related to the publication of articles based on leaked “cellphone messages that have embarrassed prosecutors and tarnished the image of an anti-corruption task force,” The New York Times reported.

Greenwald, a resident of Brazil who was born in the United States, is a co-founding editor of The Intercept. The Intercept called the charges politically motivated, saying that Brazil’s prosecutors are trying to criminalize a wide range of journalism. The charges stem from an Intercept series published in June 2019, which the news organization said was “based on a massive archive of previously undisclosed materials—including private chats, audio recordings, videos, photos, court proceedings, and other documentation—provided to us by an anonymous source.”

The prosecution of Greenwald is “apparent retaliation for The Intercept’s critical reporting on abuses committed by Justice Minister [Sérgio] Moro and several federal prosecutors,” the news organization also said in a statement provided to Ars and other media.

Greenwald has not been arrested, but prosecutors released a 95-page criminal complaint that claimed Greenwald did more than simply publish leaked information. The Times summarized the complaint:

> *Citing intercepted messages between Mr. Greenwald and the hackers, prosecutors say the journalist played a “clear role in facilitating the commission of a crime.”*
>
> *For instance, prosecutors contend that Mr. Greenwald encouraged the hackers to delete archives that had already been shared with The Intercept Brasil, in order to cover their tracks.*
>
> *Prosecutors also say that Mr. Greenwald was communicating with the hackers while they were actively monitoring private chats on Telegram, a messaging app.*

The criminal charges were not a total surprise. After The Intercept stories were published, Brazil President Jair Bolsonaro “left little doubt that he’d relish seeing the journalist punished,” the Times wrote. “In late July, the president used a derisive term to refer to Mr. Greenwald and said the journalist ‘might wind up in jail.'”

Brazil criticized for attack on press freedom

The Intercept’s statement said that Bolsonaro’s government “has repeatedly made it clear that it does not believe in basic press freedoms.” The Intercept also said that police

found no wrongdoing by Greenwald when they examined the same evidence that resulted in today's charges:

> *The evidence cited today by Brazil's Public Ministry is the same that was rigorously analyzed by the country's Federal Police, leading the agency to conclude that Greenwald did not commit any crimes in his contacts with the alleged source of our Secret Brazil Archive stories. Glenn Greenwald was not formally investigated by the Federal Police, but they concluded that there was no indication of wrongdoing committed by him.*

The charges are "an attempt to criminalize not only our journalism but also that of the dozens of partners who collaborated with our staff in over 95 stories based on the archives," The Intercept further said.

Journalists and press-freedom advocates criticized Brazil.

"Journalism is not a crime, and these charges against Glenn Greenwald are an outrage and a threat to press freedom," Washington Post media columnist Margaret Sullivan wrote on Twitter.

Freedom of the Press Foundation Executive Director Trevor Timm said that Greenwald "has bravely fought for journalistic freedom throughout his entire career. These sham charges are a sickening escalation of the Bolsonaro administration's authoritarian attacks on press freedom and the rule of law."

A Freedom House summary of press freedom in Brazil said that "politicians frequently invoke restrictive laws to silence journalists or media outlets." Reporters Without Borders ranked Brazil 105th out of 180 countries in its 2019 World Press Freedom Index. Norway, Finland, and Sweden led the ranking, while the United States was ranked 48th.

“Outrageous”

Even those who’ve had sharp disagreements with Greenwald were disturbed by the charges.

“Glenn Greenwald has called me a ‘deceitful’ mouthpiece of the national security state and I assure you I’ve rarely had a nice thing to say about him. But this is an outrageous assault on press freedom that should alarm every American,” Lawfare Executive Editor Susan Hennessey wrote.

Mike Masnick of TechDirt also noted his disagreements with Greenwald while calling Brazil’s action “a blatant attack on press freedom.”

The American Civil Liberties Union urged the US government to “immediately condemn this outrageous assault on the freedom of the press, and recognize that its attacks on press freedoms at home have consequences for American journalists doing their jobs abroad.”

As a reporter at The Guardian, Greenwald in 2013 published a series of reports based on classified US National Security Agency documents leaked by Edward Snowden. Greenwald left The Guardian in late 2013 to start The Intercept.

https://arstechnica.com/?p=1646859

Reuters: Apple cut backup end-to-end encryption plans

after FBI complained

Enlarge / The iPhone 11, iPhone 11 Pro, and iPhone 11 Pro Max running iOS 13.
Samuel Axon

reader comments

138 with 84 posters participating

Share this story

Two years ago, Apple dropped a plan that would have made it impossible for the company to decrypt iPhone and iPad backups for law enforcement, according to a Reuters report today. Reuters wrote that “six sources familiar with the matter” confirmed that Apple dropped the end-to-end encryption plan for iCloud Backup “after the FBI complained that the move would harm investigations.”

Apple had “told the FBI that it planned to offer users end-to-end encryption when storing their phone data on iCloud” more than two years ago, Reuters wrote.

“Under that plan, primarily designed to thwart hackers, Apple would no longer have a key to unlock the encrypted data, meaning it would not be able to turn material over to authorities in a readable form even under court order,” the report continued.

But the FBI objected, and Apple dropped the plan, although the exact reason for doing so isn’t clear. One former Apple employee told Reuters that the company “decided they weren’t going to poke the bear anymore.” However, another former Apple employee “said it was possible the encryption project was dropped for other reasons, such as concern that more customers

would find themselves locked out of their data more often."

Apple had "10 or so experts" working on the end-to-end encryption plan, "variously code-named Plesio and KeyDrop," but told them to stop work on the project once the decision was made, according to Reuters' sources.

The reversal "shows how much Apple has been willing to help US law enforcement and intelligence agencies, despite taking a harder line in high-profile legal disputes with the government and casting itself as a defender of its customers' information," Reuters wrote.

We contacted Apple about the Reuters report today and will update this article if we get a response.

Encryption vs. end-to-end encryption

Nearly all types of iCloud data are encrypted both in transit and on Apple's servers, Apple explains in this security overview. But only certain Apple services get the extra protection of end-to-end encryption, in which "your data is protected with a key derived from information unique to your device, combined with your device passcode, which only you know." When end-to-end encryption is enabled, Apple doesn't have a key to unlock the data and therefore cannot turn a decrypted version over to law enforcement. "No one else can access or read this data," Apple's website says.

The iCloud Keychain password manager, Wi-Fi passwords, and Siri usage information are among the data sets stored in iCloud with end-to-end encryption. Notably, Apple has not implemented end-to-end encryption for iCloud Backup, the service that lets customers back up their iPhones and iPads to Apple servers, or for iCloud Drive. The iCloud Backup and iCloud Drive data sets are encrypted at rest and in transit,

but Apple has the key to unlock them and can thus give decrypted versions to law enforcement.

Messages is a special case. Messages itself has end-to-end encryption, but iCloud Backup "includes a copy of the key protecting your Messages." If you want full protection for Messages, you'd want to disable iCloud Backup and back your iOS devices up to iTunes on your computer instead.

iCloud Backup's inclusion of a copy of the Messages key "ensures you can recover your Messages if you lose access to iCloud Keychain and your trusted devices," Apple explains. "When you turn off iCloud Backup, a new key is generated on your device to protect future messages and isn't stored by Apple."

US/Apple dispute

Apple has been one of the leading proponents of encryption in the face of government pressure to install backdoors that could undermine security for all technology users.

The Reuters report comes amid the latest dispute over encryption between Apple and the US government, which began with the FBI asking Apple for help decrypting two iPhones believed to have belonged to Mohammed Saeed Alshamrani, a Saudi Air Force officer and suspect in the December 2019 shooting of three members of the US Navy at a base in Pensacola, Florida.

As we wrote last week, "an Apple spokesperson said that Apple had provided the contents of the cloud backups of those devices to investigators within hours of the shooting, and Apple executives thought the FBI was satisfied with that—until the FBI came back a week ago and asked for additional assistance."

President Trump blasted Apple on Twitter last week, writing

that Apple “refuse[s] to unlock phones used by killers, drug dealers and other violent criminal elements.”

Apple countered that it gave the FBI “gigabytes of information,” including “iCloud backups, account information and transactional data for multiple accounts.”

Apple may be unable to unlock the phones since it hasn’t granted the government’s request for a backdoor—and continues to argue that encryption backdoors would harm security for all users.

“We have always maintained there is no such thing as a backdoor just for the good guys,” Apple said in its statement, according to CNBC. “Backdoors can also be exploited by those who threaten our national security and the data security of our customers. Today, law enforcement has access to more data than ever before in history, so Americans do not have to choose between weakening encryption and solving investigations. We feel strongly encryption is vital to protecting our country and our users’ data.”

https://arstechnica.com/?p=1646661

Boeing seeks $10 billion in loans as 737 Max crisis continues

Enlarge / Boeing 737 Max planes.

reader comments

133 with 79 posters participating, including story author

Share this story

Boeing is aiming to borrow $10 billion or more to help it get through the 737 Max crisis, CNBC reported today, citing people familiar with the matter.

“The company has secured at least $6 billion from banks so far, the people said, and is talking to other lenders for more contributions,” CNBC wrote. Citigroup, Bank of America, Wells Fargo, and JPMorgan already agreed to loan Boeing money.

A Boeing 737 Max crash killed 189 people in October 2018 and another crash killed 159 people in March 2019. The US Federal Aviation Administration and governments from around the world ordered the grounding of 737 Max planes after the March crash.

The planes are still grounded as Boeing has struggled to fix its flight-control software, known as the Maneuvering Characteristics Augmentation System (MCAS). The latest software problem was reported Friday; Boeing said it was “making necessary updates and working with the FAA on submission of this change, and keeping our customers and suppliers informed.”

Boeing’s debt load has already increased substantially over the past year. Boeing had $20.3 billion in long-term debt as of September 30, 2019, nearly double the $10.7 billion of long-term debt it had on December 31, 2018, according to a Boeing SEC filing. By contrast, Boeing added less than $1 billion in long-term debt in all of 2017.

Boeing’s short-term debt and the “current portion of [its] long-term debt” added together was $4.4 billion as of September 30. Boeing declined to comment on the $10 billion in new debt when contacted by Ars.

Big revenue drop

Boeing in October reported Q3 2019 revenue of $20 billion, down from $25.1 billion year-over-year. Revenue for the first nine months of 2019 was $58.6 billion, down 19 percent year-over-year. Net earnings in Q3 2019 were $1.2 billion, down from $2.4 billion in Q3 2018.

In July 2019, Boeing announced an after-tax charge of $4.9 billion to cover “potential concessions and other considerations to customers for disruptions related to the 737 MAX grounding and associated delivery delays.”

CNBC described Boeing’s planned $10 billion loan as a two-year, delayed-draw loan that it “can tap into it later, a move that may not immediately affect its credit rating as another type of loan or a bond would.”

Boeing fired CEO Dennis Muilenburg in December 2019 and replaced him with former board chairman David Calhoun.

https://arstechnica.com/?p=1646269

As attacks begin, Citrix ships patch for VPN vulnerability

Igor Golovniov/SOPA Images/LightRocket via Getty Images

reader comments

22 with 20 posters participating

Share this story

On January 19, Citrix released some permanent fixes to a vulnerability on the company's Citrix Application Delivery Controller (ADC) and Citrix Gateway virtual private network servers that allowed an attacker to remotely execute code on the gateway without needing a login. The vulnerability affects tens of thousands of known VPN servers, including at least 260 VPN servers associated with US federal, state, and local government agencies—including at least one site operated by the US Army.

The patches are for versions 11.1 and 12.0 of the products, formerly marketed under the NetScaler name. Other patches will be available on January 24. These patches follow instructions for temporary fixes the company provided to deflect the crafted requests associated with the vulnerability, which could be used by an attacker to gain access to the networks protected by the VPNs.

Fermin J. Serna, chief information security officer at Citrix, announced the fixes in a blog post on Sunday. At the same time, Serna revealed that the vulnerability—and the patches being released—also applied to Citrix ADC and Citrix Gateway Virtual Appliances hosted on virtual machines on all commercially available virtualization platforms, as well as those hosted in Azure, Amazon Web Services, Google Compute Platform, and Citrix Service Delivery Appliances (SDXs).

Lots to patch

That makes for lots of work over the next few weeks for Citrix customers, which include thousands of government agencies, educational institutions, hospitals, and major corporations

worldwide.

As of last week, according to data provided by Bad Packets to Ars Technica, over 26,000 servers were still vulnerable to the crafted request. The data, including information on potentially vulnerable government VPN gateways, was shared by Bad Packets with the Cybersecurity and Infrastructure Security Agency. They included a gateway associated with a DOD civilian personnel system, the US Census service, and a number of local law enforcement agencies.

Inevitably, hundreds of Citrix VPN servers will remain vulnerable for weeks or months. Some are already being attacked, according to reports from FireEye—with one attacker installing the mitigation settings to keep other attackers out and booting any other installed malware before setting up their own backdoor.

Many of the exploits thus far have installed low-impact malware, including cryptocurrency mining software. But based on what happened with last year's Pulse Secure vulnerability, ransomware operators and other cybercriminals will soon join the hunt.

Meanwhile, a member of the group operating the REvil ransomware campaign recently acknowledged that the group had attacked Travelex using the Pulse Secure vulnerability, according to security researcher Vitali Kremez. UNKN, the administrator of the REvil malware, claimed credit for the Travelex attack in a forum post on January 7 and said that Travelex executives needed to hurry up and pay, or customers' birth dates, Social Security numbers, and credit card data "would be sold to someone."

https://arstechnica.com/?p=1645999

Frontier, an ISP in 29 states, plans to file for bankruptcy

Enlarge / A Frontier Communications service van.

reader comments

159 with 99 posters participating

Share this story

Frontier Communications is planning to file for bankruptcy within two months, Bloomberg reported last week.

The telco “is asking creditors to help craft a turnaround deal that includes filing for bankruptcy by the middle of March, according to people with knowledge of the matter,” Bloomberg wrote.

Frontier CEO Bernie Han and other company executives “met with creditors and advisers Thursday and told them the company wants to negotiate a pre-packaged agreement before $356 million of debt payments come due March 15,” the report said. The move would likely involve Chapter 11 bankruptcy to let Frontier “keep operating without interruption of telephone and broadband service to its customers.”

Frontier reported having $16.3 billion in long-term debt as of September 30, 2019.

We contacted Frontier about the report of its bankruptcy plan and will update this story if we get a response.

Frontier offers residential and business services in 29 states over its fiber and copper networks. Frontier offers broadband, TV, and phone services and reported revenue of $2 billion and a net loss of $345 million in the most recent quarter.

Frontier has been losing customers and reducing its staff. Its residential-customer base dropped from 4.15 million to 3.81 million in the 12-month period ending September 30, 2019, including a loss of 90,000 customers in the most recent quarter. Also in that 12-month period, Frontier's business-customer base declined from 422,000 to 381,000.

Meanwhile, Frontier had 19,132 employees as of September 30, 2019, down from 21,375 one year earlier.

Frontier's financial performance last year was so bad that it refused to take any questions from investors during its quarterly earnings call in August. Frontier is in the process of selling its operations in Washington, Oregon, Idaho, and Montana to WaveDivision Capital.

Many customer problems

Frontier's decline is partly due to the decreasing relevance of its copper networks and its failure to properly maintain those old phone lines. But Frontier has also provided poor customer service on its modern fiber networks.

Subscribers suffered outages immediately after Frontier's 2014 purchase of AT&T's wireline network in Connecticut and Frontier's 2016 purchase of Verizon's FiOS and DSL networks in California, Florida, and Texas.

Frontier Communications failed to properly maintain its telecom network in Minnesota, leading to "frequent and

lengthy” phone and Internet outages, an investigation by the state Commerce Department found in January 2019. The investigation led to a settlement. New York state officials are also investigating Frontier over its repeated outages and long repair times.

Many Frontier customers in different states have been hit with giant overcharges and cancellation fees, or draconian policies like one requiring customers to pay for router rentals even when they have purchased their own router. (A new US law scheduled to take effect in June 2020 would ban that practice.)

Windstream, a telco that offers service in 18 states, filed for bankruptcy in February 2019. Windstream in November 2019 said its latest quarterly revenue was “$1.27 billion compared to $1.38 billion in the same period a year ago.”

https://arstechnica.com/?p=1645973

Biden wants Sec. 230 gone, calls tech “totally irresponsible,” “little creeps”

Enlarge / Former Vice President Joe Biden poking at a mobile phone in October 2019.

reader comments

34 with 24 posters participating

Share this story

Former Vice President Joe Biden is calling for one of the primary laws defining how Internet content is regulated to be "revoked," adding that the "little creeps" who run some of Silicon Valley's biggest businesses aren't the economic powerhouses they think they are.

"I've never been a fan of Facebook, as you probably know. I've never been a big [Facebook CEO Mark] Zuckerberg fan," Biden began in response to tech questions posed by The New York Times. "I think he's a real problem."

"He [Zuckerberg] knows better," Biden elaborated, telling the Times, "Not only should we be worrying about the concentration of power, we should be worried about the lack of privacy and them being exempt."

The exemption to which Biden was referring is § 230 of the Communications Decency Act. The key part of the law reads:

> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*

At its most basic level, the law draws a line between the platform that hosts content and the generator of the content hosted on it. If something is hinky in a YouTube video, "Google" isn't the company that spoke the contents; the video creator is.

"Section 230 reform" has something of a rallying cry among the far right in recent months. Sen. Josh Hawley (R-Mo.) last year introduced legislation seeking to amend the law, revoking "the immunity big tech companies receive under Section 230 unless

they submit to an external audit that proves by clear and convincing evidence that their algorithms and content-removal practices are politically neutral."

Hawley has company in both chambers of Congress. Sens. Lindsey Graham (R-S.C.) and Ted Cruz (R-Tex.) have also lent public support to the idea of Section 230 reform, as has Rep. Matt Gaetz (R-Fla.) on the House side.

The cry for reform is not limited to a single party, though. House Speaker Nancy Pelosi (D-Calif.) told Recode last April that section 230 is "a gift" to the tech firms, adding, "I don't think they are treating it with the respect that they should, and so I think that could be a question mark and in jeopardy."

Biden, however, did not call for reforms—he called for abolishing the provision entirely. "You're not exempt," he told his interviewers. "[The Times] can't write something you know to be false and be exempt from being sued. But he can. The idea that it's a tech company is that Section 230 should be revoked, immediately should be revoked, number one. For Zuckerberg and other platforms."

When the NYT pointed out that Section 230 is foundational to the modern Internet, Biden agreed, then continued:

> *And it should be revoked. It should be revoked because it is not merely an internet company. It is propagating falsehoods they know to be false, and we should be setting standards not unlike the Europeans are doing relative to privacy. You guys still have editors. I'm sitting with them. Not a joke. There is no editorial impact at all on Facebook. None. None whatsoever. It's irresponsible. It's totally irresponsible.*

It’s apparently personal, but not criminal

Biden called particular, but oblique, attention to Facebook’s decision not to block political ads that mislead users or tell outright lies, so long as those ads do not engage in obvious attempts at voter suppression. That discussion was kicked off in October, when the Trump campaign aired ads on Facebook making false accusations about Biden. The ads contained baseless claims about Biden’s activities in Ukraine and elsewhere that have been repeatedly debunked by both media outlets and also other Republican politicians.

Biden suggested to the NYT that Facebook’s choice to allow such ads could amount to defamation, saying that Zuckerberg “should be submitted to civil liability and his company to civil liability, just like you would be here at The New York Times” if the paper were to run demonstrably false stories. Whether Facebook should face any kind of criminal penalties, he added, is less clear.

If Zuckerberg or anyone else at Facebook “engaged in something and amounted to collusion that in fact caused harm that would in fact be equal to a criminal offense, that’s a different issue,” Biden added. “That’s possible. That’s possible it could happen. Zuckerberg finally took down those ads that Russia was running. All those bots about me. They’re no longer being run,” he continued. Biden seemingly conflated action taken by an opposing campaign with the kind of foreign disinformation action that is indeed rampant across social media.

The tech sector, and Facebook in particular, is overdue for some government intervention, Biden added, drawing a line through history:

> *The fact is, in every other revolution that we’ve had*

> *technologically, it's taken somewhere between six years and a generation for a government to come in and level the playing field again. All of a sudden, remember the Luddites smashing the machinery in the Midlands? That was their answer when the culture was changing. Same thing with television. Same thing before that with radio. Same thing, but this is gigantic.*
>
> *And it's a responsibility of government to make sure it is not abused. Not abused. And so this is one of those areas where I think it's being abused. For example, the idea that he cooperates with knowing that Russia was engaged in dealing with using the internet, I mean using their platform, to try to undermine American elections. That's close to criminal.*

Intuiting that Biden was still talking about Facebook, the Times interviewer posited that Zuckerberg might not have known at the time how deeply involved Russia was. "He'd argue it and I don't believe him for a second," Biden replied. "Nor do you, in your heart."

Tech on blast

Biden's antipathy for tech did not stop with Facebook; he spoke more widely of his distaste with the sector as well.

"You may recall the criticism I got for meeting with the leaders in Silicon Valley, when I was trying to work out an agreement dealing with them protecting intellectual property for artists in the United States of America," Biden said. "At one point, one of the little creeps sitting around that table, who was a multi—close to a billionaire—who told me he was an artist because he was able to come up with games to teach you how to kill people."

The interviewer asked Biden if he meant video games, and Biden agreed. He went on to say that he was "lectured" at that table by a "senior leader" who claimed that if Biden and Sen.

Patrick Leahy (D-Vt.) moved forward with the bill in question, “they would blow up the network, figuratively speaking. Have everybody contact. They get out and go out and contact the switchboard, just blow it up.”

Biden went on to say that there were representatives of seven firms sitting in that meeting, “everyone’s there but Microsoft,” and he found “you have fewer people on your payroll than all the losses that General Motors just faced in the last quarter, of employees. So don’t lecture me about how you’ve created all this employment.”

It is unclear which particular meeting with “little creeps” Biden was alluding to. The references to GM and to intellectual property, however, seem to indicate this meeting took place in 2008, while Biden was still representing Delaware in the Senate. Once he became Vice President in 2009, Biden continued to be deeply involved in copyright law struggles. Early in the first Obama term, Biden promised strong enforcement to the recording industries, and he was a key presence in a 2010 White House push to reform copyright enforcement.

While it’s hard to work out the relative economic importance of seven unknown companies that might have been represented at an unknown meeting more than a decade ago, there is no doubt that here in 2020, the tech sector is a massive contributor to the US economy. Four publicly traded companies in US history have passed the $1 trillion valuation mark. Apple was the first to do so, in 2018. Amazon followed later that year, and Microsoft joined the club in 2019. The most recent, Google parent company Alphabet, did so earlier this week.

https://arstechnica.com/?p=1645167

WeLeakInfo gets pwned by FBI; Dutch, Irish police arrest alleged breach brokers

Enlarge / The seizure notice for WeLeakInfo even included the site’s logo. Fancy.

reader comments

37 with 31 posters participating

Share this story

On Wednesday, police in the Netherlands and Northern Ireland arrested two 22-year-old men believed to be connected to WeLeakInfo, a site offering usernames and passwords from multiple data breaches for sale. At the same time, the Federal Bureau of Investigation, in coordination with the UK’s National Crime Agency, the Netherlands National Police Corps, the German Bundeskriminalamt, and the Police Service of Northern Ireland, took down the domain for the site, redirecting it to a seizure notice (shown above).

At first, some thought the takedown was simply a breach of the site itself—mostly because the FBI took the time to add the site’s logo to the takedown notice.

> *There’s a mess happening over at We Leak Info since yesterday. It looks like they got hacked, and someone threw up an FBI seizure page. The seizure notice doesn’t look legit.*
>
> *… Not a good look for them…https://t.co/XGGIRaJKQk #WeLeakInfo #WLI pic.twitter.com/SUzaAQD8Pd*

> — Cypher (@CryptoCypher) January 16, 2020

But on Thursday afternoon, the Justice Department announced the takedown and put out a call for further information on WeLeakInfo and its operators. WeLeakInfo claimed to have over 12 billion usernames and passwords from a collection of over 10,000 data breaches. Originally hosted at a Canadian hosting company's data center when set up in 2016, the domain was moved behind Cloudflare a day later. The site, originally advertised as "the most extensive private database search engine," purported to be a legitimate tool for companies to perform security research—even claiming to offer an application interface for performing bulk checks for breaches of company accounts.

Enlarge / How WeLeakInfo looked before the takedown.

But the site was alleged to be selling more than just breach warnings. In an announcement of the seizure of the domain posted Thursday by the US Justice Department, the DOJ alleged that WeLeakInfo allowed its users to access "a search engine to review and obtain the personal information illegally obtained in over 10,000 data breaches containing over 12 billion indexed records—including, for example, names, email

addresses, usernames, phone numbers, and passwords for online accounts.” The site’s subscription plans allowed users unlimited access to the data.

While the domain has been seized and computers connected to its operation were confiscated by Dutch police, the fate of the site’s server remains unknown.

https://arstechnica.com/?p=1645251

FBI arrests man suspected of orchestrating dozens of “swatting” calls

reader comments

121 with 88 posters participating

Share this story

The US government has criminally charged a Virginia man for helping to organize dozens of “swatting” attacks and bomb threats made against a variety of targets in the United States and Canada. The man allegedly belonged to a group that coordinated via IRC and Tor hidden services to target prominent gamers, journalists, and government officials.

John William Kirby Kelley.
Alexandria Sheriff’s Office

The group’s online chats were often racist, with comments suggesting antipathy toward Jews and black people. In one case, the group made a fake bomb threat to the Alfred Street Baptist Church, a predominantly African American church in Alexandria, Virginia.

Security reporter Brian Krebs was one of the first to report on the arrest of defendant John William Kirby Kelley. Krebs was the target of a swatting call he believes was organized by the group.

Kelley allegedly did research for the group, identifying possible targets and suggesting that others make calls. He also helped maintain the group’s infrastructure, according to the FBI.

Kelley was identified by authorities after he called in a bomb threat to his own school. While he blocked his own number during that call, he later made a second call to the police without properly blocking his number. Investigators realized that the two calls might be connected, questioned Kelley, and eventually got a warrant to search his devices. Police quickly

found videos, chats, and other records Kelley had saved documenting his involvement in other hoax calls, the FBI says. They also found recruiting material for Atomwaffen, a violent white supremacist group.

A story from Vice illustrates the real human costs of this kind of "prank." In 2018, Kelley's group allegedly swatted prominent gamer Andrea Rovenski. As a result, she and her mother (who lived in the same house) were thrown on the ground by police. Rovenski lost sleep over the incident, and she believes her mother paid a much higher price.

"Less than two months later, Rovenski's mother suffered a stroke—something Rovenski believes is connected to the extremely stressful event—and never fully recovered," Vice's Mack Lamoureux writes.

Other swatting incidents have had even more devastating consequences. In 2017, a Kansas man was shot to death by police responding to a swatting call. The man who made that call was sentenced to 20 years in prison last year.

While Kelley is now in custody, two other suspects are still at large, according to the FBI. The bureau believes that these two suspects are the ones who actually made most of the calls at issue in the case. Evidently, the suspects' efforts to conceal their identities from law enforcement have been successful—at least so far.

Listing image by Onfokus | Getty Images

https://arstechnica.com/?p=1643863