Verizon to buy TracFone, expanding big carriers' control of prepaid industry

Enlarge / A monitor displaying a Verizon logo and share prices at the New York Stock Exchange on September 4, 2018.
Getty Images | Bloomberg

reader comments

57 with 42 posters participating, including story author

Share this story

Verizon today announced it has struck a deal to buy TracFone in a further consolidation of the US cellular industry.

Verizon is one of three major carriers that operate nationwide wireless networks, along with AT&T and T-Mobile (which recently bought Sprint). TracFone is the country's largest reseller of mobile service and already relies primarily on Verizon's network to provide connectivity. More than 13 million of TracFone's 21 million customers "currently rely on Verizon's wireless network through an existing wholesale agreement," Verizon's announcement said.

After the sale is completed, "all TracFone customers will have access" to the Verizon network, a Verizon fact sheet on the deal said. Verizon could try to shift existing TracFone customers to Verizon plans, as Verizon said the deal will bring "enhanced access to its industry-leading wireless network and comprehensive suite of mobility products and services to a new customer base."

The deal could also increase the number of phone models that can be purchased directly from TracFone. “Verizon consumer chief Ronan Dunne said TracFone will remain a distinct business that will benefit from access to a wider range of cellphones, smart devices and connected home products through the carrier’s ownership,” The Wall Street Journal wrote today.

TracFone is a subsidiary of América Móvil, the Mexican telecom founded by Carlos Slim. TracFone had about $8.1 billion in revenue in 2019, while Verizon reported $94.2 billion in wireless revenue for the year. (Verizon’s total revenue including non-wireless business lines was $131.9 billion.)

The Verizon/TracFone merger needs regulatory approval, and Verizon said it expects to complete the deal in the second half of 2021. The sale price is potentially almost $7 billion, consisting of $3.125 billion in cash, $3.125 billion in Verizon stock, and “up to an additional $650 million in future cash consideration related to the achievement of certain performance measures and other commercial arrangements.”

TracFone and other resellers generally provide cheaper data plans than facilities-based carriers like Verizon and do so via prepaid plans instead of the postpaid ones that make up the bulk of the big carriers’ businesses. The big carriers often own the prepaid-reseller brands themselves—for example, AT&T owns Cricket Wireless, T-Mobile owns the former MetroPCS brand, and Verizon owns Visible Wireless.

Dish also entered the prepaid market by purchasing Boost Mobile from T-Mobile, which agreed to sell the former Sprint division in order to win Department of Justice approval of its merger with Sprint. Cable companies have been launching their own reseller services, providing some new competition in that part of the wireless market.

Verizon to vault past AT&T and T-Mobile in prepaid

Verizon's prepaid business had about 4 million connections as of mid-2020, down from 4.3 million a year earlier. That's a drop in the bucket compared to Verizon's 115.9 million retail postpaid connections and far fewer than the numbers of AT&T and T-Mobile prepaid customers.

"Adding TracFone would vault [Verizon] to the top spot in the prepaid market," The Wall Street Journal wrote. "T-Mobile, owner of the Metro service, has more than 20 million prepaid customers. AT&T serves about 18 million US prepaid customers mostly through its Cricket brand."

TracFone offers service under its own name and several other brands, including Straight Talk, Simple Mobile, Total Wireless, and Net10. The company has about 850 employees and over 90,000 retail locations, including at chains Walmart, Best Buy, CVS, Dollar General, and Family Dollar.

The merger, Verizon said, "will provide more US consumers seeking value wireless plans with improved experiences and enhanced services, including fixed wireless residential broadband solutions, 5G access and expanded international calling and roaming options."

Verizon also said the deal will help it compete for low-income customers. "Verizon will continue to offer Lifeline service through TracFone and further develop its core brands, products, and distribution channels, including Straight Talk, the vast majority of whose customers operate on the Verizon network today," the merger announcement said.

TracFone is facing a potential $6 million fine, as the Federal Communications Commission recently alleged that the company obtained FCC Lifeline funding by "enroll[ing] fictitious subscriber accounts" and that it improperly received more than

$1 million in the process.

https://arstechnica.com/?p=1705863

Nvidia reportedly to acquire ARM Holdings from SoftBank for $40 billion

Enlarge / Components manufactured by ARM Holdings Plc sit inside a demonstration ARMmbed parking meter on display on the second day of Mobile World Congress (MWC) in Barcelona, Spain, on Tuesday, Feb. 28, 2017. A theme this year at the industry's annual get-together, which runs through March 2, is the Internet of Things. Photographer: Pau Barrena/Bloomberg via Getty Images
Bloomberg | Getty Images

reader comments

102 with 65 posters participating

Share this story

SoftBank is set to sell the UK's Arm Holdings to US chip company Nvidia for more than $40 billion, just four years after its founder Masayoshi Son bought the chip designer and said it would be the linchpin for the future of the Japanese technology group.

Multiple people with direct knowledge of the matter said a cash-and-stock takeover of Arm by Nvidia may be announced as

soon as Monday, and that SoftBank will become the largest shareholder in the US chip company.

The announcement of the deal hinged on SoftBank ending a messy dispute between Arm and the head of its China joint venture, Allen Wu, who earlier rebuffed an attempt to remove him and claimed legal control of the unit.

Several people close to SoftBank said the matter was now "resolved," though one person close to Mr Wu said he "remains the chairman of Arm China." A spokesperson for Mr Wu declined to comment.

The takeover values Arm above the $32 billion price that SoftBank paid for the business in 2016, a deal that was struck weeks after the UK voted to leave the European Union and prompted critics including Arm's founder to accuse the country of selling off the crown jewel of its tech sector.

While Nvidia is paying more for the asset than SoftBank did, the price also reflects the scale of Arm's underperformance under the Japanese group's ownership.

Nvidia had a market valuation of roughly similar to that of Arm's at the time of the 2016 deal, but now trades with a market value of $300 billion, or roughly 10 times the amount SoftBank paid in cash for Arm. By paying for a large portion of the deals with its own shares, it is also passing part of the risk of the transaction to SoftBank.

For Nvidia, which recently overtook Intel to become the world's most valuable chipmaker, the deal will further consolidate the US company's position at the centre of the semiconductor industry. The British chip designer's technology is starting to find broader applications beyond mobile devices, in data centres and personal computers including Apple's Macs.

Arm would transform Nvidia's product line-up, which until now

has largely focused on the high end of the chips market. Its powerful graphics processors—which are designed to handle focused, data-intensive tasks—are typically sold to PC gamers, scientific researchers and developers of artificial intelligence and self-driving cars, as well as cryptocurrency miners.

To pave the way for the deal, SoftBank reversed an earlier decision to strip out an internet-of-things business from Arm and transfer it to a new company under its control. That would have stripped Arm of what was meant to be the high-growth engine that would power it into a 5G-connected future. One person said that SoftBank made the decision because it would have put it in conflict with commitments made to the U.K. over Arm, which were agreed at the time of the 2016 deal to appease the government.

SoftBank's Vision Fund previously held a stake in Nvidia, in a rare publicly listed investment for the $100 billion fund that focuses on private technology companies, but divested all of its shares early last year. Akshay Naheta, the 39-year old SoftBank executive who spearheaded that investment, has also been heavily involved in negotiations between the Japanese conglomerate and Nvidia.

The Vision Fund, which is run by Mr Naheta's close ally and former colleague from Deutsche Bank, Rajeev Misra, controls a 25 per cent stake in Arm and will get compensated as part of the deal, another person added.

One person close to the talks said that Nvidia would make commitments to the UK government over Arm's future in Britain, where opposition politicians have recently insisted that any potential deal must safeguard British jobs.

The Wall Street Journal earlier reported on the deal's imminent announcement.

Additional reporting by Ryan McMorrow in Beijing.

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

https://arstechnica.com/?p=1705716

Political appointees demand ability to rewrite CDC case reports

Enlarge / Robert Redfield, director of the Centers for Disease Control and Prevention (CDC), listens during a House Select Subcommittee on the Coronavirus. Redfield may be finding himself trapped between scientists and political appointees.

reader comments

210 with 122 posters participating

Share this story

Covid-19 Coverage

View more stories

Political appointees in the Department of Health and Human services are objecting to reports on the COVID-19 pandemic from the Centers for Disease Control and are trying to exercise editorial control of future reports. That’s the bottom line of an extensive report from Politico that was

based on both internal emails and interviews with people in the organization. The problems apparently stem from the fact-based reports from the CDC running counter to the Trump administration's preferred narrative about the spread of the pandemic and the appropriate public health responses.

The CDC documents at issue are termed Morbidity and Mortality Weekly Report, which provide rapid summaries of the state of our knowledge about public health issues. Typically, they're the product of a CDC-backed investigation into a known issue; in the past, they've focused on things like outbreaks of food-borne illnesses. While they don't have the weight of peer-reviewed literature, they're widely considered to be scientifically reliable, and their rapid publication makes them a valuable resource for public health officials.

It's easy to see how the reports' accurate information could be viewed as counter to the preferred message of the Trump administration. Trump has made reopening schools a centerpiece of his pandemic policy, but CDC Morbidity and Mortality Weekly reports have described how SARS-CoV-2 can spread rapidly in a school-aged population, how young children can bring the disease home and pass it on to adults, and how children can suffer severe complications from the disease.

Rather than recognizing that facts aren't supportive of their policies, the administration's political appointees have apparently decided that the CDC is not presenting the facts because it's trying to undercut Trump. Politico quotes Michael Caputo, a former Trump campaign official now at Health and Human Services, as saying, "Our intention is to make sure that evidence, science-based data drives policy through this pandemic—not ulterior deep state motives in the bowels of CDC." One of the emails obtained for the story, written by another political appointee, says, "CDC to me appears to be writing hit pieces on the administration," and another accused the reports of being used to "hurt the president."

Paul Alexander, one of the few involved who has an epidemiology background, complained in another email, “CDC tried to report as if once kids get together, there will be spread and this will impact school re-opening… Very misleading by CDC and shame on them.” Yet that’s exactly what appears to be happening in many locations, suggesting the CDC has a better grasp on the issue than Alexander does.

The political staff has attempted to block the release of some of the Morbidity and Mortality reports and demanded the ability to review and edit all future reports. (Alexander, apparently unironically, suggested he needed to ensure the reports were “fair and balanced.”) While all of the planned reports were eventually published, Politico indicates that the non-scientific staff are gaining increased oversight of the reports prior to their publication.

https://arstechnica.com/?p=1705666

Defying crackdowns, QAnon continues its relentless global spread

Enlarge / BOSTON—A man wearing a QAnon vest held a flag during a No Mandatory Flu Shot Massachusetts rally held outside of the State House in Boston on Aug. 30, 2020, to demonstrate against Gov. Charlie Baker’s order for mandatory influenza vaccinations for all students under the age of 30, an effort to lower the burden on the health care system during the COVID-19 pandemic.

Boston Globe | Getty Images

reader comments

42 with 35 posters participating

Share this story

The online phenomenon known as QAnon is evolving beyond its pro-Trump roots and spreading rapidly into new global communities, despite efforts by social media platforms to stamp out the world's most persistent conspiracy theory.

Cryptic posts by the group or individual known as "Q" first began appearing on the imageboard 4chan in 2017, propagating a theory that swiftly gained traction online in which the US president is leading a battle against a "deep state" that wields control over the country.

In July, TikTok blocked several hashtags, while Twitter banned thousands of accounts. Last month, Facebook launched a sweeping crackdown on the movement, including shutting down 790 QAnon-related groups.

But adherents of QAnon have been swift to adapt to their new conditions, rebranding themselves to avoid detection and piggybacking on to related movements to further propagate their message.

"It's a meta-conspiracy—it just has so much in it you can pick and choose from, which explains its rapid spread," said Chine Labbe, European managing editor at NewsGuard, a counter-misinformation organization. "It seduces people in a lot of different circles and across ideologies."

After the shutdowns

Facebook's actions succeeded in removing some of the biggest accounts from the platform, including QAnon News and

Updates—the largest group on the site, with 200,000 members at its peak. But a range of groups from a wide variety of communities has since absorbed the newly displaced believers.

As of September 9, a search for "QAnon" on Facebook yielded 11 groups with 10,000 or more members, compared with 30 in July. One, a private group called QAnon Update Group, has more than 39,000 likes and predates the first QAnon post, with previous names referring to extraterrestrials, popular video games, and a Vietnamese marketplace.

Meanwhile, members of the closed QAnon groups have used a range of tactics to remain on the platform and continue to spread their message. Some have migrated to other areas, said Angelo Carusone, president of Media Matters for America, targeting related communities such as anti-mask groups or remnants of the Tea Party, to maintain their network on the platform.

"If [Facebook] had taken their action a year ago, you would not have seen that explosive growth [in QAnon] which began in March," said Mr. Carusone. "The core infrastructure would not have been able to scale with it."

Aoife Gallagher, a researcher at the Institute for Strategic Dialogue, a London-based think-tank, added that some QAnon believers were trying to circumvent detection, sometimes by changing their names. One group with around 3,000 followers had substituted the word Cue for the letter Q.

A spokesperson for Facebook said that the company always removes content which incites violence and had removed QAnon accounts, groups, and pages that had violated the policies in the past. They also said that they were aware that movements and groups can evolve quickly and that the platform's teams were studying attempts to avoid enforcement.

New dimensions

The social media crackdown came as QAnon had already begun to move into a range of new online communities, tweaking its message in the hope of broadening its network and capturing more adherents.

On Facebook, for instance, QAnon-related content has been posted on a number of spiritual, wellness, and alternative medicine groups. One such group, with over 90,000 members, featured memes about crystal healing, palmistry, and alien technology interspersed with QAnon-related claims about pedophilia and COVID-19 denialism.

“If you post a QAnon meme to one of these groups, they can be distributed far and wide,” said Mr. Carusone.

A newer breed of QAnon believer has emerged from these communities, said Joe Ondrak, senior researcher at Logically, a counter-misinformation organization, which he dubs “lower-case q.” Rather than the political dimension of the conspiracy theory, they are primarily focused on child sex-trafficking claims—one of the other original tenets of QAnon.

“They’re all about the narrative itself—they’re not big on personalities except when it comes to the bad guys,” he said. “It’s not the Trump cult for them—it’s about saving kids from this shadowy cabal.”

“A real knot of different narratives”

QAnon content now circulates freely on anti-child abuse groups on Facebook. Several of these were created in recent months, coinciding with QAnon-driven conspiracies about child trafficking and efforts by believers to hijack hashtags such as #SaveTheChildren.

Content in these groups ranges from genuine news reports of pedophilia and child abuse to misinformation. References are often made to the QAnon mythos, even when the wider movement is not always explicitly named. “They’re mixing fictional problems with real ones, creating a real knot of different narratives,” said Mr. Ondrak.

The problem of disentangling real and QAnon narratives has been further complicated as the movement has spilled into the real world. Logically and outlets including NBC document links between QAnon believers and organizing of global marches against child sexual abuse.

Mr. Ondrak argued that this softer-edged form of the conspiracy requires a particularly nuanced policy response to counter the spread of disinformation while avoiding penalizing genuine advocates for child safety.

Q goes global

At the same time, QAnon is increasingly shedding its US-centric focus. “Every country in the world has elites, so [QAnon advocates] manage to work these local stories to adapt the QAnon framework,” said Ms Labbe.

In France, QAnon ideas have merged with the similarly nebulous Yellow Vest movement, which began two years ago as a protest against fuel prices and the cost of living. Three of the Facebook QAnon groups with more than 10,000 members are Francophone.

According to Similar Web data, Dissept, a French conspiracy theory website created in June 2020, is the single largest site of referrals to Qmap.pub, the major dedicated QAnon website. A NewsGuard report found that, in under two months, it had reached the top 2,500 sites in France by online engagement.

Mr. Ondrak said that narratives could also adapt significantly when crossing international borders, sometimes in seemingly contradictory ways. He pointed to the co-opting of QAnon discourse by Islamophobic groups in the UK, a sentiment not usually present in its US incarnation.

“It’s this weird malleability and localization as it spreads further into Europe,” he said. “They’re folding localized prejudices into the pyramid of [QAnon beliefs].”

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

https://arstechnica.com/?p=1705648

Why online voting is harder than online banking

Justin Sullivan/Getty Images

reader comments

139 with 52 posters participating, including story author

Share this story

For a feature last week, I talked to a number of election experts and computer security researchers who argued that secure Internet voting isn’t feasible today and probably won’t be for many years to come. A common response to this argument—one that came up in comments to last week’s

article—is to compare voting to banking. After all, we regularly use the Internet to move money around the world. Why can't we use the same techniques to secure online votes?

But voting has some unique requirements that make secure online voting a particularly challenging problem.

Votes are anonymous, banking isn't

Every electronic transaction in the conventional banking system is tied to a specific sender and recipient who can confirm that a transaction is valid or raise the alarm if it isn't. Banks count on customers to periodically review their transactions—either online or in paper statements—and notify the bank if fraudulent transactions occur.

By contrast, experts told me, elections are supposed to be secret. In-person elections don't just allow voters to cast a secret ballot, they typically require them to do so. Mandatory secrecy insulates voters from coercion by bosses, abusive spouses, elder care workers, or others in positions of power or influence.

Once the voter drops a paper ballot into a ballot box, it gets mixed together with the other ballots. Not only is it hard for anyone to link a ballot back to the voter who cast it, it's also hard for the voter to prove to anyone how he or she voted.

Building a secure digital voting system with the same properties is difficult. If votes aren't linked to voter identities, there's no way for voters—or anyone else—to verify that their votes were recorded accurately.

Cryptographers have developed complex cryptographic protocols for accurately counting ballots while maintaining at least partial anonymity. But these protocols themselves are complex and difficult for ordinary voters to verify.

Some online voting companies have dealt with this challenge by dispensing with strong ballot secrecy. Voatz, for example, gives each voter an anonymized identification number that allows them to look up their votes as they were recorded on the Voatz server. This is probably essential for ensuring that votes are recorded correctly. But it erodes the sanctity of the private ballot, since people in positions of power could coerce voters into revealing how they voted.

Online banking isn't actually that secure

The more important issue, however, is that online banking systems aren't actually that secure. Indeed, conventional payment networks get compromised constantly. The Nilson Report, a financial industry trade publication, estimated that credit card fraud cost the world almost $28 billion in 2018.

A big reason for this is that banks recognize that there's a tradeoff between security and customer convenience. Strong security measures like two-factor authentication or rigorous verification of signatures would cut down on fraud but would also irritate many customers. Banks and financial networks realize that beyond a certain point, stricter controls will cost the bank more in lost customers than they save in fraud prevention. So they accept that a fair amount of fraud is a cost of doing business.

Banks' security efforts are also aided by the fact that people hacking financial networks are typically trying to divert stolen funds to themselves. Often banks can "follow the money" to figure out who was responsible for a particular hack, recovering the stolen funds and deterring others from trying a similar attack. Bank hacking is also of little interest to foreign governments, most of which have plenty of money.

Election hacking is different. We talk metaphorically about

people “stealing” votes, but someone hacking an election isn’t trying to directly profit from their hack. This means that the authorities can’t follow the money to identify suspects.

When fraudulent transactions are flagged after the fact, banks automatically credit lost funds back to customers. They try to identify the culprits and make them pay, but if that’s not possible, banks absorb the losses themselves.

This approach is totally unworkable for voting. Voting officials can’t issue voters after-the-fact credits for their stolen votes the way banks do for stolen funds. An election needs to produce a definitive result that is quickly and widely accepted as legitimate. Even a small number of fraudulent votes could flip the results of an election and destroy public confidence in the voting process. Major elections, including the American presidency, have been decided by a few hundred votes out of millions cast.

So our voting infrastructure needs to be a lot *more* secure than our online banking infrastructure. And experts say we simply don’t know how to build online systems with the necessary level of security.

https://arstechnica.com/?p=1704658

Porn surfers have a dirty secret. They’re using Internet Explorer

reader comments

71 with 60 posters participating

Share this story

They’re back—attacks that use booby-trapped Web ads to install malware on the computers of unsuspecting visitors.

So-called malvertising works by paying advertising networks to display banner ads on legitimate websites. Malicious code snuck into the ads then surreptitiously exploits vulnerabilities in browsers or browser plugins. The result: merely browsing to the wrong site infects vulnerable computers with malware that steals banking credentials, logs passwords, or spies on users.

Malvertising never went away, but it did become much less common in the past few years. Thanks to dramatic improvements in browser security, malvertising was replaced by more effective infection techniques, such as phishing, malicious macros in Microsoft Office documents, and tricking targets into installing malicious apps that masquerade as legitimate software.

Internet Exploder… really?

But over the past month, malvertising has made something of a comeback, security firm Malwarebytes reported this week. Company researchers said they recently found two different groups placing booby-trapped ads on xHamster, a site with more than 1 billion monthly visits, according to SimilarWeb. The ads redirect visitors to sites that serve malicious code. When viewed with Internet Explorer or Adobe Flash, the code can exploit critical vulnerabilities in unpatched versions of Internet Explorer.

“Threat actors still leveraging exploit kits to deliver

malware is one thing, but end users browsing with Internet Explorer is another," Malwarebytes researchers wrote. "Despite recommendations from Microsoft and security professionals, we can only witness that there are still a number of users (consumer and enterprise) worldwide that have yet to migrate to a modern and fully supported browser."

Internet Explorer has always been one of the more targeted browsers. In part, that was because of its once dominant market share. Subpar security protections, when compared to Chrome and later Firefox, was another key reason. Microsoft has since released Edge and encouraged all users to adopt it. But the software maker continues to offer IE since custom plugins and software often lock organizations and individuals into using the outdated browser.

The malvertising renaissance seems to be motivated by attackers "squeezing the last bit of juice from vulnerabilities in Internet Explorer and Flash Player (due to retire for good next year)," the Malwarebytes post observed.

Enter Fallout and RIG

xHamster visitors using IE are redirected to a malicious site that hosts content from either Fallout or RIG, two of the better known exploit kits. Exploit kits are the malware equivalent of paint-by-numbers. Sold in underground forums, they allow people with relatively modest technical skills to serve exploits that will infect visitors with malware of the buyer's choice.

The Fallout exploit kit was redirecting targets to inteca-deco[.]com, a domain that masqueraded as a Web design agency. Behind the scenes, the site redirected targets to a different domain hosting malicious content from a Fallout. It exploited IE vulnerability CVE-2019-0752 or Flash vulnerability CVE-2018-15982. Later, targets were redirected to a different domain, websolvent[.]me, which used a different redirection

trick to deliver the exploits.

When successful, the exploits installed the Raccoon Stealer. The malware, according to security firm CyberArk, sells for about $75 a week. Customers use it to steal credit card data, login credentials, cryptocurrency wallets, and other sensitive data.

A second malvertising group, often referred to as malsmoke, is also using exploit kits to install malware known as Smoke Loader. They, too, are displaying malicious ads on xHamster by purchasing space from a legitimate ad network.

“Malsmoke is probably the most persistent malvertising campaign we have seen this year,” the Malwarebytes post said. “Unlike other threat actors, this group has shown that it can rapidly switch ad networks to keep their business uninterrupted.”

Protecting yourself

With a little training, it’s not hard to spot most malvertising attacks. They usually start with being redirected from the site users were viewing to a site they don’t recognize and made no attempt to visit. Readers who find themselves in this position should close the browser and disconnect the computer from the Internet as quickly as possible. They should never click on links.

The better protection is to use a modern browser such as Edge, Firefox, Chrome, or Brave. The latter is a relatively new offering that’s built from the same Chromium engine as Chrome. All of these browsers have been hardened with security sandboxes and other protections designed to thwart malware attacks. Using IE in 2020 is reckless, whether viewing porn or any other kind of Web content.

https://arstechnica.com/?p=1705552

Trump and Twitter are on likely showdown path with expanded misinfo rules

Aurich Lawson

reader comments

52 with 39 posters participating

Share this story

With just over 50 days to go before the 2020 US presidential election, everything is—predictably—hitting the fan. Foreign interference is of course an ever present threat, with known actors both attempting to amplify social discord as well as literally hack campaigns. But good old homegrown deliberate misinformation is also a significant threat to this year's entire electoral process.

Misinformation spreads rapidly thanks to the advent of social media—especially Facebook, Google, and Twitter. Facebook already announced its (weak) plan for combating rampant falsehoods, and this week Twitter and Google both made their plans public as well.

Tweet, tweet…

Twitter's existing policy prohibits users from posting content that includes "false claims on how to participate in civic

processes” or “content that could intimidate or suppress participation.” In other words, at a very high level you’re not allowed to use Twitter to lie about voting or tell people not to vote.

False information can come from anywhere, and plenty of us have seen some spread—sometimes unwittingly—by our own friends and family online. Unfortunately, one of the most prevalent and high profile sources of false election claims has been sitting US President and 2020 candidate Donald Trump, and his favorite platform is Twitter.

Twitter first began appending fact-check labels to Trump’s tweets in May, when the president alleged that all mail-in voting is inherently fraudulent (it’s not). Twitter added a small label to the bottom of the tweets with a link, reading, “Get the facts about mail-in ballots.”

That kind of fact-check, however, is not exactly detailed or obvious, and Twitter appears to have recognized that.

“People who use our service have told us that non-specific, disputed information that could cause confusion about an election should be presented with more context,” Twitter wrote in a company blog post. So beginning September 17, Twitter will be providing a whole lot more context, and it will “label or remove false or misleading information intended to undermine public confidence in an election or other civic process.”

The list of content Twitter will now label or delete includes:

> *1. False or misleading information that causes confusion about the laws and regulations of a civic process, or officials and institutions executing those civic processes.*
>
> *2. Disputed claims that could undermine faith in the process itself, e.g. unverified information about election rigging, ballot tampering, vote tallying, or certification of election*

> *results.*
>
> *3. Misleading claims about the results or outcome of a civic process which calls for or could lead to interference with the implementation of the results of the process, e.g. claiming victory before election results have been certified, inciting unlawful conduct to prevent a peaceful transfer of power or orderly succession.*

It seems likely then to be only a matter of when, not if, the expanded policy once again puts Twitter on a collision course with the president and other high-profile administration or conservative figures. But Twitter is very clear that the policy will apply to all (even if some get warnings and others get banned). “We will not permit our service to be abused around civic processes, most importantly elections,” the post concludes. “Any attempt to do so—both foreign and domestic—will be met with strict enforcement of our rules, which are applied equally and judiciously for everyone.”

Searching for answers

Google’s new policy, meanwhile, is less about what people say and more about what people find. The company is fully aware that many of its search features, including autocomplete, can direct users to places they otherwise might not have gone. As such, it’s trying to reduce the amount of misinformation search might serve to you.

Google will be beefing up its fact checks in search, Google News, and Google Images, the company said in a blog post. So far in 2020 to date, users have seen more than four billion fact checks come up, the company says, which is more than in all of 2019.

Not all users, however, are going to Google News and looking at the helpful “fact check” and “full coverage” modules when

they seek information. So Google's also tweaking search.

"We have improved our automated systems to not show predictions if we detect that the query may not lead to reliable content," Google said, admitting that AI can't catch everything and sometimes human enforcers need to help. They're also enacting changes on election-related search queries:

> *We will remove predictions that could be interpreted as claims for or against any candidate or political party. We will also remove predictions that could be interpreted as a claim about participation in the election—like statements about voting methods, requirements, or the status of voting locations—or the integrity or legitimacy of electoral processes, such as the security of the election. What this means in practice is that predictions like "you can vote by phone" as well as "you can't vote by phone," or a prediction that says "donate to" any party or candidate, should not appear in Autocomplete.*

That said, however, anyone can still search for those terms or any others if they're willing to type out whole words instead of relying on autocomplete. And the reliability of the links anyone follows through is just as big of a grab bag as ever.

https://arstechnica.com/?p=1705487

Judge in Theranos fraud case orders 14-hour psychological

test for Holmes

Enlarge / Elizabeth Holmes, founder and former CEO of Theranos, arrives for motion hearing on Monday, November 4, 2019, at the U.S. District Court House in San Jose, California.

reader comments

163 with 114 posters participating

Share this story

Elizabeth Holmes—the disgraced founder and ex-CEO of the now-defunct blood-testing startup, Theranos—may use a mental condition as a defense against a slew of federal fraud charges, according to a court document filed this week.

Holmes and Theranos' former president Ramesh "Sunny" Balwani were charged in June 2018 with nine counts of wire fraud and two counts of conspiracy to commit wire fraud. Federal prosecutors allege the pair—who were romantically involved during the alleged crimes—engaged in conspiracy to defraud Theranos investors out of more than $100 million and defraud doctors and patients into falsely believing the company's faulty blood-testing technology could reliably perform accurate health tests with just drops of blood from a finger-prick.

According to the court document filed this week, Holmes—who is now being tried separately from Balwani—notified the court last December that she plans to submit "expert evidence relating to a mental disease or defect or any other mental condition" that has bearing on the issue of guilt. The expert providing such evidence was named in the document as

psychologist Mindy Mechanic, of California State University, Fullerton.

According to Mechanic's faculty website, she focuses on "psychosocial consequences of violence, trauma, and victimization with an emphasis on violence against women and other forms of interpersonal violence." The site also notes that Mechanic "frequently provides expert testimony in complex legal cases involving interpersonal violence."

The court document goes on to say what the specific mental health testimony will cover, but the information is redacted.

In response to Holmes' plans to provide mental health evidence, federal prosecutors requested that they should also be able to examine Holmes' mental state and provide their own psychiatric evidence in court as a fair rebuttal.

The enforcer

The judge in the case, US District Judge Edward Davila of the Northern District of California, agreed with the prosecutors. As such, he ordered Holmes to undergo up to 14 hours of psychological testing and psychiatric evaluation by two government-appointed doctors over the course of two consecutive days. Davila also ordered that the government's evaluation of Holmes be recorded on video—over Holmes' objections.

The mental condition defense is just the latest twist in the long, dramatic saga of Theranos and its darling-turned-pariah founder. Holmes, a college dropout, garnered glowing media attention after founding her startup in 2003 at the age of just 19. She was known for her Steve Jobs-like fashion choices and bold claims of technological prowess. In 2014, the company was valued at $9 billion.

But according to multiple media investigations since,

Theranos’ technology was faulty and much of the company’s claims were misleading or false. Behind the scenes, Balwani was co-leading the company with Holmes and was reportedly known around the office as “the enforcer.”

Holmes had met Balwani while they both studied Mandarin at Beijing University during the summer of 2002, when she was about 18 and he was 37. They later became romantically involved and Balwani joined the company in 2009.

Holmes’ trial is currently scheduled for March 2021 and Balwani’s trial is expected to follow. They both face up to 20 years in prison.

https://arstechnica.com/?p=1705584

Price gouging and defective products rampant on Amazon, reports find

Enlarge / Amazon’s orange-yellow logo wall.
David Ryder/Getty Images

reader comments

143 with 99 posters participating

Share this story

New reports released this week serve as a cautionary tale for

consumers who shop at Amazon, by far the largest online retailer in the US. While complaints about Amazon's third-party vendor marketplace are by now commonplace, the new reports find that not only did Amazon itself price-gouge customers during the height of the pandemic, but also that many of its white-label, Amazon-branded products are just as likely to be dangerously defective as third-party goods.

Product shortages—both for pandemic-related supplies such as masks and sanitizer and also for basic household goods such as toilet paper—hit nationwide in February, March, and April as the country shut down and everyone who could holed up at home. As tends to happen when demand skyrockets but supply doesn't, prices on a wide range of items went up. And up. And then up some more.

By March, regulators were desperately trying to stem the tide of price gouging flooding online retailers, especially Amazon's sprawling third-party Marketplace.

Amazon at the time said in a corporate blog post that it was "working hard to protect customers from bad actors" in its Marketplace. "We have suspended more than 3,900 selling accounts in our US store alone for violating our fair pricing policies," Amazon wrote on March 23, "and we've been partnering directly with law enforcement agencies to combat price gougers and hold them accountable."

Not just third parties

A new report from consumer watchdog group Public Citizen, however, finds that price-gouging for some critical goods was just as prevalent in Amazon's own first-party sales as it was in its vendor marketplace. Between May and August, for example, Public Citizen found that ordinary antibacterial hand soap, which usually sells for around $1.50, was going for $7—a 470-percent price increase.

Public Citizen's report includes two instances of markups of 1,000 percent or more: disposable face masks, which were selling for $40 instead of $4, and corn starch, which sold for $9 instead of $0.90. "It is troubling that so much effort was put into blaming third-party sellers, but so little effort was made to stop the price increases—including on the products sold by Amazon directly," the report concludes. "Amazon is not merely a victim in the price gouging on its marketplace. It is a perpetrator."

The report confirms previous findings from consumer advocacy group US PIRG looking into coronavirus-related price gouging on Amazon, including on first-party listings. A follow-up report US PIRG published this week found that "erratic pricing" for staple items such as paper towels, facial tissues, flour, and bleach still persists on Amazon today.

"We attempt to identify excessively high prices through manual and automated processes designed to detect prices that are significantly above historical pricing for the same product, taking into account reasonable cost increases experienced by sellers," Amazon spokesperson Nicole Jefferson told US PIRG about the price spikes.

It is extremely unlikely that anyone at Amazon took the time to manually go through its listings to elevate specific prices by a certain amount. The company infamously relies on dynamic, algorithmic pricing that changes constantly in response to a whole slew of conditions. An April report by The Markup found that coronavirus-related conditions were causing some particularly noticeable price volatility that Amazon did not seem to cap.

Explosive issues

Multiple deep-diving investigations in recent years have found unsafe, mislabeled, counterfeit, or fraudulent goods for sale in Amazon's third-party marketplace, which is increasingly

compared to an unsupervised flea market.

The Wall Street Journal in 2019 found that not only is some of the junk for sale in the Marketplace trash in a very literal sense but also that listings for unsafe items persist even after those goods are recalled or banned from the site.

About 60 percent of Amazon's retail sales take place through the third-party marketplace, with millions of vendors placing tens of millions of listings. At that scale, it can undoubtedly be difficult to keep up, and perhaps some errors are expected.

Amazon's own sales, however—the other 40 percent of its retail empire—increasingly rely on and promote Amazon's hundreds of private-label brands. AmazonBasics is one of the most successful of those brands. It sells the kind of product lines you'd expect to find store brands of in a Target, Walmart, or other big-box store: home goods, bed and bath products, kitchen accessories, luggage, lightbulbs, charging cables, and so on.

You might think that bringing all of those products and brands in-house and listing, selling, and shipping them as a first-party merchant would allow Amazon to exercise much tighter quality control over those goods than it does in the Marketplace. According to a new CNN report, however, you'd be wrong.

CNN identified more than 1,500 consumer reviews of AmazonBasics products that described products overheating, burning someone or something, or outright catching fire. About 30 items with "three or more" reviews describing how a product caught fire were still available for sale at the time CNN published its story. Another dozen vanished while CNN's story was in progress: "Some became unavailable after CNN began its reporting, and at least four product pages were removed from the retailer's site entirely—leaving behind dead URLs known by

employees as ‘dog pages,'” CNN wrote.

An AmazonBasics microwave, for example, featured more than 150 user reviews describing “safety concerns, including flames and smoke.” Several included pictures of the singed products. CNN obtained one of the faulty microwaves from a customer and submitted it to experts at the University of Maryland for testing.

“As soon as the researchers turned it on, the microwave began sparking and smoking, causing it to react as if its user put foil or other metal inside,” CNN wrote. A user-uploaded video included in the CNN story shows one of the microwaves sparking dangerously when a plastic bowl of macaroni and cheese is placed inside and heated.

Amazon told CNN that relying on user reviews to uncover faulty products is insufficient, saying that it also looks at sales history and customer service contacts when looking for a problem. “Using customer reviews alone to conclude a product is unsafe or imply there’s a widespread issue is misleading,” an Amazon rep told CNN in a statement. However, CNN also found at least 10 reports filed with the US Consumer Product Safety Commission (CPSC) regarding eight different dangerous or faulty AmazonBasics products. Amazon, however, has only ever conducted two official recalls on AmazonBasics goods.

https://arstechnica.com/?p=1705350

Russian state hackers are

targeting Biden and Trump campaigns, MSFT warns

Enlarge / Vladimir Putin.

reader comments

1 with 1 posters participating

Share this story

Fancy Bear—the Russian state hacking group that brought you the smash-and-leak attacks on the Democratic National Committee and World Anti-Doping Agency, the NotPetya worm that inflicted billions of dollars of damage worldwide, and the VPN Filter compromise of 500,000 routers—is targeting organizations involved in elections taking place in the US and UK, Microsoft has warned.

Over a two-week period last month, the group attempted attacks on more than 6,900 accounts belonging to 28 organizations, Microsoft said. Between September 2019 and last June, Fancy Bear targeted tens of thousands of accounts belonging to employees of more than 200 organizations. The hackers use two techniques—one known as "brute forcing" and the other called "password spraying"—in an attempt to obtain targets' Office365 login credentials. So far, none of the attacks has succeeded.

Security researchers from a host of companies widely agree that Fancy Bear works on behalf of the GRU, Russia's military intelligence agency. The GRU has been tied to more than a decade of advanced hacking campaigns, including several that have inflicted serious damage to national security. Industry members use an assortment of colorful names to refer to the

group. Besides Fancy Bear, there's also Pawn Storm, Sofacy, Sednit, and Tsar Team. Microsoft's name for the outfit is Strontium.

"Microsoft's Threat Intelligence Center (MSTIC) has observed a series of attacks conducted by Strontium between September 2019 and today," Microsoft Corporate Vice President Tom Burt wrote in a post published on Thursday. "Similar to what we observed in 2016, Strontium is launching campaigns to harvest people's log-in credentials or compromise their accounts, presumably to aid in intelligence gathering or disruption operations."

Strontium is one of three state-sponsored hacking groups that Microsoft said are targeting the 2020 elections. Zirconium—believed to work for the People's Republic of China—has been targeting "high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community." Phosphorus, which researchers say works on behalf of the Islamic Republic of Iran, continues to target personal accounts of people associated with President Donald Trump's reelection campaign.

Big bad bear

While campaigns from all three groups pose a risk, the one from Fancy Bear carries the biggest threat, given the group's advanced skill and techniques and its track record of brazen and dangerous hacks. An accompanying Microsoft post that provided technical details about the Fancy Bear hacking campaign said the group has streamlined and automated its operations significantly since 2016.

Four years ago, Fancy Bear leaned heavily on spear phishing, or the sending of convincing-looking emails that spoofed personnel from Google or other well-known organizations. The emails, one that famously hooked Hillary Clinton's

presidential campaign chairman, John Podesta, falsely reported to receivers that their accounts had been compromised. The spearphishes then instructed them to log in to what turned out to be a fake site and change their passwords.

Now, Fancy Bear is relying primarily on tools that perform password spraying and brute forcing. The change makes it easier to operate at scale and in a way that's more anonymized. The tools are distributed through a pool of roughly 1,100 IP addresses, with most of them belonging to the Tor anonymization service. In Thursday's technical post, Microsoft researchers wrote:

> *This pool of infrastructure has evolved over time, with an average of approximately 20 IPs added and removed from it per day. STRONTIUM's tooling alternates its authentication attempts amongst this pool of IPs approximately once per second. Considering the breadth and speed of this technique, it seems likely that STRONTIUM has adapted its tooling to use an anonymizer service to obfuscate its activity, evade tracking, and avoid attribution.*

Spreading the load

In the attacks between August 19 and September 3, Microsoft observed a daily average of 1,294 IP addresses from more than 500 address blocks and 250 autonomous system numbers. Some of the netblocks were used more often than others. The overutilization of the netblocks created an opportunity for researchers to ferret out Fancy Bear activity that used the anonymization service. Microsoft used this Azure Sentinel query to identify failed authentication attempts from the three most widely used address blocks and group them by the user agents attempting to log in.

The two techniques Fancy Bear is using are:

- Password spraying, which attempts to find valid username-password combinations. Typically, there are about four tries each hour over the course of days or weeks. Almost every attempt originates from a different IP address.
- Brute-forcing, which peppers a targeted account with about 300 login attempts per hour over the course of several hours or days.

What, me worry?

Given the fallout from Fancy Bear's 2016 hacks, you might think that most high-value targets had since adopted multifactor authentication, which requires the person logging in to provide the correct password and to also prove possession of a device or present a fingerprint or other biometric. But according to Microsoft, you'd be wrong. Figures the company published last October show that less than 10 percent of large-organization accounts use any form of MFA. Turning multifactor authentication on thwarts most credential-harvesting attacks, Microsoft said.

Thursday's technical post also recommended high-value target organizations monitor logs for failed authentications.

"When monitoring login activity in your accounts, look for any type of discernible patterns in these failed authentications and track them over time," researchers advised. Password spray is an increasingly common tactic of nation-state actors."

https://arstechnica.com/?p=1705249