Google, Apple, and Mozilla block Kazakhstan government’s browser spying

Getty Images | Thomas Jackson

reader comments

40 with 36 posters participating

Share this story

Major browser makers are blocking the use of a root certificate that Kazakhstan’s government has used to intercept Internet traffic.

Mozilla and Google issued a joint announcement today saying that “the companies deployed technical solutions within Firefox and Chrome to block the Kazakhstan government’s ability to intercept Internet traffic within the country.” Each company is deploying “a technical solution unique to its browser,” they said.

Apple told Ars that it is also blocking the ability to use the certificate to intercept Internet traffic.

Kazakhstan reportedly said it halted the use of the certificate. But the browser makers’ actions could protect users who already installed it or prevent future use of the certificate by Kazakhstan’s government.

Mozilla and Google said they took the action in response to “credible reports that Internet service providers in Kazakhstan have required people in the country to download and

install a government-issued certificate on all devices and in every browser in order to access the Internet." The certificate "allowed the [Kazakhstan] government to decrypt and read anything a user types or posts, including intercepting their account information and passwords," the companies wrote. "This targeted people visiting popular sites Facebook, Twitter, and Google, among others."

Certificate blocked after installation

Mozilla explained in another post that the Kazakhstan root certificate "will not be trusted by Firefox even if the user has installed it."

"We believe this is the appropriate response because users in Kazakhstan are not being given a meaningful choice over whether to install the certificate and because this attack undermines the integrity of a critical network security mechanism," Mozilla said. The company also encouraged Internet users in Kazakhstan to "research the use of virtual private network (VPN) software, or the Tor Browser, to access the Web."

Similarly, Google said that "Chrome will be blocking the certificate the Kazakhstan government required users to install" and that "no action is needed by users to be protected."

Google added the certificate to CRLSets, which Chrome uses to "quickly block certificates in emergency situations."

Moreover, Google said that "the certificate will be added to a blocklist in the Chromium source code and thus should be included in other Chromium based browsers in due course."

Mozilla doesn't "take actions like this lightly, but protecting our users and the integrity of the Web is the

reason Firefox exists," Mozilla Senior Director of Trust and Security Marshall Erwin said.

Chrome Senior Engineering Director Parisa Tabriz said that Google "will never tolerate any attempt, by any organization—government or otherwise—to compromise Chrome users' data."

When contacted by Ars, Apple said it is blocking the certificate so that it cannot be used to intercept Internet traffic even after a user has installed it.

"Apple believes privacy is a fundamental human right, and we design every Apple product from the ground up to protect personal information," Apple also said in a statement to Ars and other media outlets. "We have taken action to ensure the certificate is not trusted by Safari and our users are protected from this issue." This covers Safari for both iOS and MacOS, Apple told Ars.

Edge and Internet Explorer

The situation with Microsoft is a bit murkier.

Microsoft, the maker of Edge and Internet Explorer, told Motherboard that "The Certificate Authority (CA) in question is not a trusted CA in our Trusted Root Program." That means the certificate will not be installed by default, but a browser user could choose to install it.

Not trusting the certificate isn't necessarily enough to prevent users from being spied on, though. A Censored Planet report from July 23 that Mozilla and Google referred to said, "The CA is not trusted by browsers by default, and must be installed manually by a user."

But Internet users in Kazakhstan "cannot access affected sites at all if they do not install the root certificate for the fake CA and allow interception," the report said.

Microsoft not trusting the certificate might make it a bit harder for users to install it. But if Microsoft isn't blocking the ability to spy on users after the certificate has been installed, they wouldn't be protected like users of other browsers.

On the plus side, Microsoft is in the process of switching Edge to a Chromium back-end, so Edge would eventually get the protection built into Chromium. But the Chromium-based Edge is still in beta.

We asked Microsoft about how it's handling the Kazakhstan certificate and will update this article if we get a response.

Update: Microsoft gave us the same statement it previously gave to Motherboard, but provided no response to our question about whether it is doing anything to block the ability to spy on users after the certificate has been installed.

Kazakhstan prez: "There are no grounds for concerns"

A Reuters story on August 7 said that "Kazakhstan has halted the implementation of an Internet surveillance system criticized by lawyers as illegal, with the government describing its initial rollout as a test."

State security officials claimed they were trying to protect people in Kazakhstan from "hacker attacks, online fraud and other kinds of cyber threats," Reuters wrote.

Kazakhstan President Kassym-Jomart Tokayev "said in a tweet he had personally ordered the test which showed that protective measures 'would not inconvenience Kazakh Internet users,'" Reuters wrote. "There are no grounds for concerns," Tokayev also said.

The Mozilla/Google post noted that this was "not the first

attempt by the Kazakhstan government to intercept the Internet traffic of everyone in the country."

The companies wrote:

> *In 2015, the Kazakhstan government attempted to have a root certificate included in Mozilla's trusted root store program. After it was discovered that they were intending to use the certificate to intercept user data, Mozilla denied the request. Shortly after, the government forced citizens to manually install its certificate but that attempt failed after organizations took legal action.*

https://arstechnica.com/?p=1555809

Ring asks police not to tell public how its law enforcement backend works

Enlarge / Your local police might like to interest you in this product.

reader comments

168 with 93 posters participating

Share this story

Amazon's Ring line of consumer home surveillance products enjoys an extensive partnership with local police departments

all over the country. Cops receive free product, extensive coaching, and pre-approved marketing lines, and Amazon gets access to your 911 data and gets to spread its network of security cameras all over the nation. According to a trio of new reports, though, the benefits to police go even further than was previously known—as long as they don't use the word "surveillance," that is.

Gizmodo on Monday published an email exchange between the chief of police in one New Jersey town and Ring showing that Ring edited out certain key terms of a draft press release before the town published it, as the company frequently does.

The town of Ewing, New Jersey, in March said it would be using Ring's Neighbors app. Neighbors does not require a Ring device to use; consumers who don't have footage to share can still view certain categories of crime reports in their area and contribute reports of their own, sort of like a Nextdoor on steroids.

Law enforcement has access to a companion portal that allows police to see an approximate map of active Ring cameras in a given area and request footage from them in the course of an investigation. The town also launched a subsidy program, giving up to 200 residents a $100 discount on the purchase of Ring security products. Members of the police department also received $50 discount vouchers for their own use.

The original draft press release, obtained by Gizmodo, showed that the town used one of Ring's pre-written press release templates and inserted a quote from the chief of police that read, in part, "Security cameras have been proven to be essential in deterring crime, and surveillance systems have assisted in closing cases that may have otherwise gone unsolved."

Ring approved a version with that sentence edited out, telling Ewing police the company avoids using the terms "surveillance"

or “security cameras” because that might “confuse residents into thinking this program requires a Ring device or other system to participate or that it provides any sort of direct access to user devices and information.”

If it quacks like a duck…

Police may not be allowed to use the words “surveillance” or “security cameras” in their marketing copy, but another pair of new reports highlights the significant surveillance capabilities Ring-branded security cameras can provide to law enforcement.

Local police departments have asked Ring to share “names, home addresses, and email addresses” of everyone who purchases a subsidized Ring device, Vice Motherboard reported yesterday, with some apparent success.

Email exchanges and other documents Motherboard obtained from several localities show that in at least three cities, Ring had the capability to share a list of everyone who used a city subsidy to purchase a camera, theoretically to prevent homeowners from double-dipping.

In Arcadia, California, the company told city government that it would “provide the City with an address report for the products purchased in order to help the Arcadia Police Department track the location of Ring Video Doorbells and other Ring security camera equipment, and assess the level of community interest.”

“We have names of all the people who purchased if you want to block these people,” a Ring employee added in an email exchange with an Arcadia government employee. “We will match against names and emails of everyone who purchased at the event and prevent people from doubling up.”

A spokesperson for Arcadia told Motherboard that the city did

not request a registry, nor have one in its possession. Ring also told Motherboard it “does not provide, and has never provided, resident information to law enforcement or cities participating in Ring’s subsidy match program” and said the statements Motherboard read were a “misrepresentation.”

Elsewhere in California, Motherboard found, Ring’s subsidy program contract with Rancho Palos Verdes includes a requirement that, for three years following completion of services, Ring must provide the city with “ledgers, books of accounts, invoices, vouchers, canceled checks, reports, studies,” as well as “all drawings, specifications, maps, designs, photographs, studies, surveys, data, notes, computer files, reports, records, documents and other materials” upon request. The company also told the city that it tracks the names, email addresses, and home addresses of everyone who buys a subsidized camera and places those addresses on a map to ensure they all fall within the city limits.

Ring told Motherboard that it both does and does not create maps of consumers who buy subsidized cameras, confirming that it does so in order to check against the city limits but adds that it has “never created a map of everyone who used an online promo code as part of the subsidy program.”

A Ring representative contacted Ars after the publication of this story to dispute Motherboard’s reporting. The spokesperson said that Ring does not provide customer information to law enforcement partners, “period,” but also added that Ring device owners “submit their information knowing it will be used to verify their residency for the Ring subsidy program” and that the address verification process on the city end “allows Ring to cross reference residents who participate in a subsidy event with an official City record to determine eligibility” based on the agreement between Ring and the city.

Hush-hush

Ring device owners are often unclear on what information, specifically, police can see and how they can use it. That secrecy is entirely by design, CNET reports today, as Ring has a list of features its police partners are explicitly not supposed to share with the public.

Documents security researcher Shreyas Gandlur obtained through a FOIA request include a communication from Ring to police in Bensenville, Illinois, saying that “Neighbors Portal back-end features should not be shared with the public, including the law enforcement portal on desktop view, the heat map, sample video request emails, or the video request process itself as they often contain sensitive investigative information.”

CNET rounded up all of the information it could gather on those features from a combination of its own and others’ previous reporting, FOIA requests, and interviews with police. Among the features CNET describes in detail is the process through which police can request footage from local Ring users.

For example, as part of an investigation into an auto theft, Bensenville police on July 11 sent a request for footage in a specific neighborhood taken in a 10-hour window between 8:00pm on July 9 and 6:00am on July 10. Users who received the request were presented with a big blue button reading, “Share your Ring videos now” or a smaller text option beneath to “check your Ring videos before sharing.”

Users who decline to share footage through the app may have police showing up at their door asking them to share in person if online requests don’t work out. Law enforcement can also go to Amazon directly with a valid legal demand and bypass the user’s consent to access the footage entirely.

https://arstechnica.com/?p=1555505

Facebook audit of alleged anti-conservative bias fails to pinpoint any

reader comments

92 with 74 posters participating

Share this story

Following years of accusations that it stifles right-wing speech, Facebook has published an audit failing to show any particular anti-conservative bias, and some conservatives are furious.

Law firm Covington & Burling LLP conducted the audit under the auspices of former Sen. John Kyl, a Republican who served in the US Senate representing Arizona from 1995-2013 and again for several months in 2018 following the death of Republican Sen. John McCain. The interim report (PDF), released today, seeks to reconcile the different ways Facebook sorts and presents content to its billions of users with users' perception of biased or quashed material.

Conservative politicians have for years been complaining that Facebook suppresses right-wing speech, despite nonpartisan data showing that conservative outlet Fox News is far and away the biggest English-language publisher on Facebook by user engagement. Fellow right-wing outlets Daily Wire and Breitbart

also feature prominently among the top sites by engagement, mixed in among mainstream news outlets such as NBC, the BBC, CBS, and The New York Times.

Claims about alleged anti-conservative bias on social media have reached new heights in recent months, with the Trump administration and the president himself amplifying the allegations. The White House held a social media summit in July, at which Trump lambasted “the tremendous dishonesty, bias, discrimination, and suppression” practiced by Twitter, Facebook, and Google.

The audit

As “conservative” is an imprecise and flexible term, former Sen. Kyl writes, the report considered the extremely broad umbrella of “political conservatives, people of orthodox religious views, libertarians, pro-lifers, traditionalists, Republicans, and free-speech advocates.” From that pool, Covington identified 133 persons to interview in 2018, then conducted follow-up interviews in 2019.

The report generally puts the concerns interviewees identified into one of six overall buckets, such as content enforcement or ad policies. But by and large, the most frequent problem identified in every category is one of transparency. Respondents felt that the algorithms Facebook used to surface content were unclear and the mechanisms behind efforts to reduce spam “too opaque.”

Similarly, interviewees complained about Facebook’s hate-speech designations and policies, both objecting to the entire category of “hate speech” existing in the terms of service and also objecting to how organizations are categorized as “terrorist groups or hate organizations,” which are prohibited on the platform. They also took issue with the way Facebook flags content as violating one of its policies and the completely unclear and occasionally seemingly arbitrary

process for appealing a takedown.

Some complaints in the report, such as the claim that fact-checking by organizations such as the Associated Press and PolitiFact skews to the left, definitely espouse a conservative point of view. Complaints about Facebook's lack of transparency and seemingly inconsistent or arbitrary enforcement of its rules, however, have for many years been coming from all sides.

The conclusion

"Freedom of expression undergirds the First Amendment," Kyl writes in his conclusion, as well as being considered a basic human right by the United Nations. But for all the complaints identified by participants in the research, the report does not actually identify any specific or consistent bias.

"Facebook's policies and their application have the potential to restrict free expression," Kyl notes. "Given the platform's popularity and ubiquity, this is a danger that must be taken seriously." The platform has made some baby steps toward transparency that help, he concludes, but "[t]here is still significant work to be done to satisfy the concerns we heard from conservatives."

"While we err on the side of free speech, there are critical exceptions: we don't allow content that might encourage offline harm or is intended to intimidate, exclude, or silence people," Facebook communications VP Nick Clegg wrote in a company blog post. "And we work to slow and reduce the spread of content like debunked hoaxes and clickbait by downranking it in News Feed. We know we need to listen more as we work to strike the right balance with these policies."

Facebook might have hoped having a staunch conservative oversee the audit and write the report would mitigate criticism by Republicans. It did not. Sen. Josh Hawley (R-Mo.)

said in a statement that the report wasn’t a genuine audit. Instead, he called it “a smokescreen disguised as a solution.”

“Facebook should conduct an actual audit by giving a trusted third-party access to its algorithm, its key documents, and its content-moderation protocols,” Hawley added. “Then Facebook should release the results to the public.”

The Media Research Center, a conservative organization, criticized the report, saying it “stunningly fails to admit fault or wrongdoing,” and that any changes made by Facebook to date toward addressing the complaints levied by conservatives are “empty and insulting.”

Nor was the report met with open arms by left-leaning groups. The Center for American Progress told Politico the report was a “lurid fiction perpetuated within right-wing circles,” adding, “Facebook made a grave mistake in allowing external political actors to direct an assessment of company policy and practices.”

https://arstechnica.com/?p=1555017

How malformed packets caused CenturyLink’s 37-hour, nationwide outage

reader comments

60 with 46 posters participating, including story author

Share this story

CenturyLink’s nationwide, 37-hour outage in December 2018 disrupted 911 service for millions of Americans and prevented completion of at least 886 calls to 911, a new Federal Communications Commission report said.

Back in December, FCC Chairman Ajit Pai called the outage on CenturyLink’s fiber network “completely unacceptable” and vowed to investigate. The FCC released the findings from its investigation today, describing how CenturyLink failed to follow best practices that could have prevented the outage. But Pai still hasn’t announced any punishment of CenturyLink.

The outage was so extensive that it affected numerous other network operators that connect with CenturyLink, including Comcast and Verizon, the FCC report said. An FCC summary said:

> *The outage affected communications service providers, businesses customers, and consumers who relied upon CenturyLink’s transport services, which route communications traffic from various providers to locations across the country. The outage resulted in extensive disruptions to phone and broadband service, including 911 calling. As many as 22 million customers across 39 states were affected, including approximately 17 million customers across 29 states who lacked reliable access to 911. At least 886 calls to 911 were not delivered.*

The 37-hour outage began on December 27 and “was caused by an equipment failure that was exacerbated by a network configuration error,” the FCC said. CenturyLink estimates that more than 12.1 million phone calls on its network “were blocked or degraded due to the incident,” the FCC said.

Additionally, about 1.1 million of CenturyLink's DSL customers lost service for parts of the 37 hours. Another 2.6 million DSL customers "may have experienced degraded service," the FCC said.

Pai today again called the outage "completely unacceptable" and said "it's important for communications providers to take heed of the lessons learned from this incident."

But the FCC didn't announce a punishment or even an order requiring CenturyLink to take specific steps to upgrade its network. Instead, the FCC said it "will engage in stakeholder outreach to promote best practices and contact other major transport providers to discuss their network practices," and "offer its assistance to smaller providers to help ensure that our nation's communications networks remain robust, reliable, and resilient." The FCC said it will also issue a public notice "reminding companies of industry-accepted best practices."

We asked Pai's office today if he's planning any disciplinary action against CenturyLink, and we will update this article if we get a response.

While Pai's FCC deregulated broadband when it repealed net neutrality rules, it still regulates landline phone networks such as CenturyLink's with its Title II authority over common carriers.

When contacted by Ars, Democratic FCC Commissioner Jessica Rosenworcel said the report should have been completed sooner and that it should have included "an action plan to avoid a repeat. It's a real problem [that] there is no such plan here."

Root cause

Problems began the morning of December 27 when "a switching

module in CenturyLink's Denver, Colorado, node spontaneously generated four malformed management packets," the FCC report said.

CenturyLink and Infinera, the vendor that supplied the node, told the FCC that "they do not know how or why the malformed packets were generated."

Malformed packets "are usually discarded immediately due to characteristics that indicate that the packets are invalid," but that didn't happen in this case, the FCC report explained:

> *In this instance, the malformed packets included fragments of valid network management packets that are typically generated. Each malformed packet shared four attributes that contributed to the outage: 1) a broadcast destination address, meaning that the packet was directed to be sent to all connected devices; 2) a valid header and valid checksum; 3) no expiration time, meaning that the packet would not be dropped for being created too long ago; and 4) a size larger than 64 bytes.*

The switching module sent these malformed packets "as network management instructions to a line module," and the packets "were delivered to all connected nodes," the FCC said. Each node that received the packet then "retransmitted the packet to all its connected nodes."

The report continued:

> *Each connected node continued to retransmit the malformed packets across the proprietary management channel to each node with which it connected because the packets appeared valid and did not have an expiration time. This process repeated indefinitely.*
>
> *The exponentially increasing transmittal of malformed packets resulted in a never-ending feedback loop that consumed*

> *processing power in the affected nodes, which in turn disrupted the ability of the nodes to maintain internal synchronization. Specifically, instructions to output line modules would lose synchronization when instructions were sent to a pair of line modules, but only one line module actually received the message. Without this internal synchronization, the nodes' capacity to route and transmit data failed. As these nodes failed, the result was multiple outages across CenturyLink's network.*

Restoration and changes for the future

CenturyLink became aware of the outage at 3:56am ET, and by mid-morning it had "dispatched network engineers to Omaha, Neb., and Kansas City, Mo., to log in to affected nodes directly." They traced the problem back to the Denver node. At 9:02pm, the company "identified and removed the module that had generated the malformed packets."

But the outage continued because "the malformed packets continued to replicate and transit the network, generating more packets as they echoed from node to node," the FCC wrote. Just after midnight, at least 20 hours after the problem began, CenturyLink engineers "began instructing nodes to no longer acknowledge the malformed packets." They also "disabled the proprietary management channel, preventing it from further transmitting the malformed packets."

"Much of the network" was functioning normally by 5:07am ET on December 28, but not all nodes were restored until 11:36pm that night.

Even after all nodes were restored, "some customers experienced residual effects of the outage as CenturyLink continued to reset affected line modules and replace line

modules that failed to reset," the FCC said. CenturyLink determined that the network had "stabilized" by 12:01pm on December 29.

Best practices not followed

The FCC report said that several best practices could have prevented the outage or lessened its negative effects. For example, the FCC said that CenturyLink and other network operators should disable system features that are not in use.

"In this case, the proprietary management channel was enabled by default so that it could be used if needed," the FCC wrote. "While CenturyLink did not intend to use the feature, CenturyLink left it unconfigured and enabled. Leaving the channel enabled created a vulnerability in the network that, in this case, contributed to the outage by allowing malformed packets to be continually rebroadcast across the network."

The report also said that CenturyLink could have used stronger filtering to prevent the malformed packets from propagating. CenturyLink used filters "designed to only mitigate specific risks." Instead, CenturyLink could have used "catch-all filters" that only allow expected traffic.

CenturyLink also should have set up "memory and processor utilization alarms" in its network monitoring, the FCC said. Even though the malformed packets "quickly overwhelmed the processing capacity of the nodes," this "did not trigger" any alarms in CenturyLink's system.

After the incident, CenturyLink "replaced the faulty switching module and shipped it to Infinera to perform a forensic analysis," the FCC wrote. Infinera engineers still haven't been able to replicate the problem, but the companies "have taken additional steps to prevent a repeat of this particular outage," the FCC said.

Those additional steps include CenturyLink disabling the proprietary management channel. “Infinera has disabled the channel on new nodes for CenturyLink’s network and has updated the node’s product manual to recommend disabling the channel if it is to remain unused,” the FCC said.

The report continued:

> *The service provider and vendor also established a network monitoring plan for network management events to detect similar events more quickly. Currently, CenturyLink is in the process of updating its nodes’ Ethernet policer to reduce the chance of the transmission of a malformed packet in the future. The improved Ethernet policer quickly identifies and terminates invalid packets, preventing propagation into the network. This work is expected to be complete in fall 2019.*

When contacted by Ars today, CenturyLink said that the “outage was caused by a network management card that generated malformed packets that unfortunately were retransmitted across parts of CenturyLink’s transport network.”

CenturyLink further said that it “has taken a variety of steps to help prevent the issue from reoccurring, including disabling the communication channel these malformed packets traversed during the event and enhancing network monitoring. We value our customers and regret any inconvenience this event may have caused.”

Impact on Comcast, Verizon, and more

The outage had “rippling effects” on other providers that rely on CenturyLink’s long-haul transport network, the FCC said.

“The outage potentially affected 3,552,495 of Comcast’s VoIP customers for 49 hours and 32 minutes,” with Comcast phone

customers potentially experiencing “a fast-busy signal or diminished call quality if calls were transmitted over affected transport facilities,” the FCC said.

The outage also disrupted Comcast’s ability to route 911 calls in Idaho.

Verizon uses CenturyLink’s network to transport portions of its wireless network traffic, and the “outage affected Verizon Wireless’s network across several Western states, including intermittent service problems in one county in Arizona, 12 counties in Montana, 21 counties in New Mexico, and four counties in Wyoming,” the FCC said.

“In Arizona and New Mexico, this outage potentially affected 314,883 users of Verizon Wireless’ network and resulted in 12,838,697 blocked calls (based on historical data),” the FCC said.

Tens of thousands of Verizon customers on Verizon’s CDMA network would have been unable to dial 911 during the outage, the FCC said. 911 service on Verizon LTE was unaffected “because the LTE network does not use the affected CenturyLink network for transport,” the FCC said.

The CenturyLink outage also had major impacts on TeleCommunication Systems (a 911 provider), Transaction Network Services (which provides SS7 service for TeleCommunication Systems and other small network providers), General Dynamics Information Technology (a 911 provider), and West Safety Services (another 911 provider).

“The CenturyLink outage also had smaller effects on other service providers,” the FCC said. These smaller effects had an impact on millions of people, though. The FCC wrote:

> *AT&T estimates that 1,778,250 users may have been affected. Some of the potential effects include dropped calls, voice service degradation, and callers receiving fast-busy signals*

> *when calling. TDS reported that 1,114 of its wireline users may have been affected. 911 call delivery was also affected for several service providers. Bluegrass Cellular, in Kentucky, reported that the outage potentially affected 911 call delivery for 195,384 wireless users. Cellcom, a Wisconsin-based wireless provider, notified the Commission that 53 calls to 911 were transmitted without ANI [Automatic Number Identification] and ALI [Automatic Location Identification]. Cox reported that the outage potentially affected 654,452 VoIP users. In Iowa, US Cellular reported that the outage potentially affected ALI for 911 calls for 94,380 of its wireless users. None of the providers or PSAPs [public-safety answering points] reported any harms to life or property due to the outage.*

https://arstechnica.com/?p=1554119

What does Amazon’s “Top Brand” badge actually mean?

Getty Images | Leon Neal

reader comments

78 with 64 posters participating

Share this story

Amazon’s biggest asset can also be a headache for its customers. The so-called “everything store” really *does* sell

almost any item consumers might want, but it’s often cumbersome and time-consuming to sort through them all. To avoid “choice overload,” the retail giant has come up with certain signals designed to help people distinguish high-quality products from the rest. They include star ratings and product reviews, as well as “Amazon’s Choice,” a mysterious badge bestowed on some individual items, which has recently become the subject of scrutiny from lawmakers. Now, Amazon is testing a new signifier, called “Top Brand.” But no one seems to know what, exactly, a “Top Brand” is, and Amazon won’t say.

Amazon has long given customers the ability to search by “Top Brands,” but the products previously weren’t distinguished by a special badge in search results. Now, if you search for “swimming goggles,” for instance, Amazon may return several pairs from Speedo whose photos bear a “Top Brand” badge. Here’s the weird part: the longstanding “Top Brands” search filter isn’t *quite* the same thing as the newer “Top Brand” badge. Here’s an example: if you look up “women’s belts” on Amazon and filter for “Top Brands,” you may notice that not all of the results actually receive the Top Brand badge. How can a company be a Top Brand in one sense but not in another?

Louise Matsakis via Amazon

Amazon says the discrepancy exists because the Top Brand badge is only a feature within Amazon Fashion, the part of its website dedicated to clothes, accessories, and luggage, while the Top Brands search filter is available across the entire marketplace. It makes sense for Amazon to try out this new badge feature specifically for fashion, since consumers are generally brand-conscious when shopping for things like handbags and shoes. But since not all women’s belts are within the fashion category, they’re not eligible for the Top Brand badge, even though Amazon might consider them to be Top Brands generally. Confusing, right?

At this point in the story, you may be wondering: What even *is*

a Top Brand? Are Top Brands selected by humans? Or is the metric controlled by an algorithm? Amazon, for its part, says the Top Brand badge simply highlights brands that customers love, but it did not go into any further detail about how that’s determined.

Louise Matsakis via Amazon

Wired reached out to four Amazon experts to ask about the logic behind the preexisting Top Brands filter, including two former employees, and they each had different explanations. Fred Dimyan, the CEO of Potoo Solutions, a firm that consultants with e-commerce companies, says Amazon takes two factors into consideration when awarding the honor: the amount of products a brand sells and how many different products it

offers in the first place. In other words, companies that make a narrow range of goods, but sell a lot of them, are likely to be Top Brands. Dave Bryant, an Amazon seller and blogger, thinks the distinction might be related to customers' overall purchase satisfaction, which can include metrics like how often people returned items.

James Thomson, a former Amazon employee and a partner at Buy Box Experts, a firm that consults with independent Amazon sellers, says Top Brands likely have high sales volumes and high conversion rates, meaning a lot of people who look at their product listings ultimately choose to buy from them. Chris McCabe, another former Amazon employee who now consults with Amazon sellers at eCommerceChris.com, says Top Brands are the highest revenue-earning items in a certain category. Every expert agreed that "Top Brand" is not a promotional title companies can pay to display on their Amazon product listings.

At least anecdotally, Top Brands look to encompass household names you might find in a mall, like Steve Madden, Oakley, Under Armour, and IZOD. That might be the point: to flag the names you're already familiar with from shopping in brick-and-mortar stores, so it's easier to purchase something quickly from a trusted company. "I wouldn't be surprised if the idea is to make this function like being verified on social platforms," says Juozas Kaziukénas, founder of the e-commerce intelligence firm Marketplace Pulse, who first alerted Wired to the Top Brand badge. But there are also lots of unknown companies with the Top Brand distinction, and every one of Amazon's in-house labels appears to be designated a Top Brand, too.

After Wired reached out to Amazon for this story, something strange happened. Many of the Top Brand badges that had been present in search results Wired conducted disappeared,

including in an incognito browsing window on several different computers, browsers, and phones. Amazon says, because the feature is a test, it may not always be visible.

US lawmakers have begun scrutinizing how Amazon evaluates the goods for sale in its sprawling marketplace using signals like Top Brand. On Monday, Senator Bob Menendez and Senator Richard Blumenthal, both Democrats, sent a letter to Amazon CEO Jeff Bezos asking for a "detailed explanation" about how the Amazon's Choice badge is awarded, after a Buzzfeed investigation found it was sometimes given to what appeared to poor-quality items. Democratic presidential candidate and Massachusetts Senator Elizabeth Warren has also expressed concern that Amazon may favor items from its own house brands over those from competitors. And the Department of Justice and Federal Trade Commission each recently announced they are looking at the business practices of online marketplaces, including Amazon specifically.

In a statement, a spokesperson for Amazon didn't respond directly to the senators' letter. The company instead highlighted its efforts to detect fake product reviews and said it believes that 90% of inauthentic reviews are computer-generated.

Opaque features like "Top Brand" serve as a reminder that Amazon isn't a traditional retailer, despite the fact that it often wants to *look* like one to consumers. It's an enormous marketplace where millions of independent merchants from around the world sell their goods. Amazon needs not just to combat bad actors but also steer customers toward the brands it knows they're likely to be happy with, or risk them getting overwhelmed and going somewhere else. The hard part for Amazon, like every online platform, is figuring out how to manage the chaos without taking full responsibility for the consequences of its management choices.

Is there something about Amazon you think we should know?

Contact the author at louise_matsakis@wired.com or via Signal at 347-966-3806.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1553261

Surprise! Uber and Lyft don’t like NYC’s new ride-hail rules

Enlarge / The Uber ride-sharing app is seen on a mobile phone on February 12, 2018.

reader comments

84 with 55 posters participating

Share this story

Uber CEO Dara Khosrowshahi, who took the helm of the controversial company back in 2017, is known for being pretty unflappable. He was even upbeat during the company’s second quarter earnings call, when he was charged with explaining why Uber posted more than $5 billion in losses in just a few months’ time.

But in response to one analyst’s question, about how the regulations in New York had affected the company’s bottom line, Khosrowshahi got a bit spicy, at least for Khosrowshahi.

“I think anyone who tells you that the changes in New York City are good is…” he trailed off for a moment. “It’s malarkey, frankly.”

One person’s malarkey is another’s sensible policy decision. Nearly a decade after ride-hail companies began exploiting the gray areas of decades-old taxi regulations around the country, Uber and Lyft have found themselves subject to increasingly strict rules in the Big Apple.

The city, its Democratic presidential hopeful mayor, Bill De Blasio, and its ride-hail regulator in chief, the Taxi and Limousine Commission, say the rules are aimed at helping drivers and at cutting down on city traffic, which has slowed to a jog’s pace in some parts of Manhattan. The companies say the regulations hurt drivers, riders, and of course, their bottom line. Drivers, meanwhile, say *they’re* left holding the bag.

The new wave of rule-passing started last summer, when the city instituted the country’s first-ever freeze on for-hire vehicle licenses, barring drivers from registering new cars to drive for the companies. (The freeze exempts wheelchair-accessible and electric vehicles.) In January, Uber and Lyft trips beginning or ending in much of Manhattan got slapped with an extra $2.75 congestion charge. (Taxis got a $2.50 surcharge of their own.) Then, despite a lawsuit from Lyft (and a smaller competitor named Juno), the companies were forced to begin paying drivers $17.22 per hour earlier this year. And a new state law will force the companies to rejigger their fleets to accommodate wheelchair using-passengers more quickly. Phew.

Now, new rules approved by city regulators this month extend the freeze on new Uber and Lyft vehicle licenses in New York

indefinitely. (This spring, a judge blocked an Uber lawsuit aimed at stopping it). The rules also cut down on “cruising,” or the time drivers spend waiting for their next rides or driving to their customers, forcing the companies to again rethink how they’re dispatching drivers.

The regulations are particularly less than ideal for the companies—malarkey, some might say—because the city is among their largest markets. In filings with the US Securities and Exchange Commission just before it went public, Uber said New York is one of five metro areas that collectively account for just under a quarter of its gross ride-hail bookings. (The others are Los Angeles, San Francisco, London, and São Paulo.) Though Lyft did not disclose a similar metric in its own public filings, the company is still mostly US-based, suggesting its New York business may be even more important.

The city has symbolic importance, too. Though most other cities don’t have the authority to regulate ride-hail in the way that New York does, many, also sick of traffic, are looking for ways to do so. Some hope to levy fees on the companies, like the kind collected in Chicago, Washington, DC, and, if San Franciscoans decide to pass an upcoming ballot measure, the City by the Bay. Others are attracted to the hard stick of New York’s ride-hail vehicle cap. In the run up to her election, Chicago’s new mayor told a newspaper that she would favor new limits on the number of ride-hail vehicles in the city. (The city’s consumer protection office, which is in charge of regulating ride-hail, did not respond to WIRED’s request for comment.)

Uber and Lyft, for their part, argue they’re unfairly scapegoated for a traffic problem that can mostly be traced back to regular-old Americans driving their regular-old cars to work alone every day. “The TLC’s misguided policies will reduce New Yorkers’ access to affordable and reliable transportation,” Lyft spokesperson Campbell Matthews said in a statement, while an Uber spokesperson said the company worries

“that the Mayor’s rules will hurt drivers’ ability to earn a living.”

The ride-hail companies have responded to the rules, which they say have been instituted too quickly for anyone to understand their effect, with cat-and-mouse tactics aimed at keeping riders in cars *and* revenues in pocket. The companies have, for example, raised prices across the city, a move that Uber says has led to stunted ride growth in some low-income neighborhoods.

The ride-hail companies are also changing the way their apps work for New York City drivers, many of whom work full-time because of the city’s more stringent licensing policies. Now, in times of low demand, Lyft limits the number of drivers on the road, giving priority to high-volume drivers who have accepted and completed 90% of their rides, or those who have wheelchair-accessible cars, or those participate in the company’s Express Drive program, which rents vehicles to licensed drivers who don’t own cars. The driver app also now includes a “heat map” showing where rides are in the highest demand, and Lyft has urged drivers searching for rides to go there before turning on their app—urging them, essentially, to drive to where the app needs them without being paid for it, and without Lyft being penalized by both the new driver wage and new cruising rules. Uber sent an email to drivers earlier this month indicating it is also mulling changes to its driver app.

Many drivers are displeased. In a letter sent to the Taxi and Limousine Commission in June, the Independent Drivers Guild, which says it represents 65,000 drivers, urged the city to take action against Lyft for the changes it had made to its app. (The IDG is backed by the International Association of Machinists but funded, in part, by Uber.) “The app companies treat us like disposables,” driver and IDG member Tina Raveneau told the Taxi and Limousine Commission during testimony in June. The IDG also opposes New York’s decision to

extend its vehicle license cap, suggesting that, caught in the middle, drivers feel there is plenty of blame to go around.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1552661

Apple sues company that sells “perfect replicas” of iOS without a license

Enlarge / An image from Apple’s lawsuit shows a real iPhone X and Corellium’s service running a virtual iPhone X.

reader comments

60 with 47 posters participating

Share this story

Apple yesterday sued Corellium, a company that sells access to virtual machines that run copies of the operating system used in iPhones and iPads.

Corellium markets iOS virtualization as “a research tool for those trying to discover security vulnerabilities and other flaws in Apple’s software,” according to Apple’s complaint (PDF) filed in US District Court for the Southern District of Florida. But “Corellium’s true goal is profiting off its blatant infringement,” Apple wrote. “Far from

assisting in *fixing* vulnerabilities, Corellium encourages its users to sell any discovered information on the open market to the highest bidder."

Corellium offers access to copies of iOS in a cloud service and in private installations on a customer's premises, with the latter costing $1 million a year, the lawsuit said. "Corellium does so with no license or permission from Apple," the lawsuit said.

Corellium says on its Twitter account that it is the "first and only platform to offer iOS, Android, and Linux virtualization on ARM," and that it is not merely a "simulator." Corellium tweets also touted the ability "to run virtual iPhones in the cloud" and "run any version of iOS." With Corellium virtualization, "It's possible to pause, rewind, and fast-forward everything that's done on the [virtual iOS] device… whilst Corellium reveals the internal code to help hackers discover what went wrong (or right) when they started tinkering," according to a Forbes article from February 2018.

"Straightforward" copyright case

Apple's lawsuit touted its own commitment to security research, writing that it "has never pursued legal action against a security researcher" and that the company offers up to $1 million per security report to researchers through its bug bounty programs. "Apple has also announced that it will provide custom versions of the iPhone to legitimate security researchers to allow them to conduct research on Apple devices and software," the lawsuit said.

Corellium, by contrast, "makes no effort whatsoever to confine use of its product to good-faith research and testing of iOS," Apple wrote. Apple quoted one of Corellium's founders, Chris Wade, as saying on a podcast that researchers who find security flaws "might want to keep it to themselves, because

it will be worth a lot of money to a lot of people."

But Apple's case doesn't rely solely on its claim that Corellium's goals are less than noble. According to Apple, "This is a straightforward case of infringement of highly valuable copyrighted works."

Apple's lawsuit continued:

> *Corellium's conduct plainly infringes Apple's copyrights. This is not a case in which it is questionable or unclear whether the defendant reproduced the rights-owner's works, or more subtly, whether particular portions of the works that the defendant took are ultimately protected by federal copyright law. Instead, Corellium has simply copied everything: the code, the graphical user interface, the icons—all of it, in exacting detail.*
>
> *Corellium explicitly markets its product as one that allows the creation of "virtual" Apple devices. For a million dollars a year, Corellium will even deliver a "private" installation of its product to any buyer. There is no basis for Corellium to be selling a product that allows the creation of avowedly perfect replicas of Apple's devices to anyone willing to pay.*

Corellium has touted its product "as an alternative to purchasing 'jailbroken iPhones on eBay,'" Apple's lawsuit said. Corellium also publicly acknowledged "that it had given access to its platform to the developers of an iOS exploit called 'unc0ver,' so the developers could test the exploit 'on any device running any firmware.' Within weeks, those developers released a new exploit of iOS 12," Apple said. Unc0ver lets iPhone users jailbreak their phones.

Apple's complaint further argued:

> *Corellium has no plausible defense to these acts of copyright*

> *infringement. On information and belief, Corellium is indiscriminately marketing the Corellium Apple Product to any customer, including foreign governments and commercial enterprises. Corellium is not selectively limiting its customers to only those with some socially beneficial purpose and/or those who promise to use Apple's copyrighted works, through the Corellium Apple Product, only in lawful ways (though it is highly doubtful whether, under the circumstances, such uses actually exist). Instead, Corellium is simply unleashing Apple's copyrighted works for the world-at-large to use, period.*

Apple is seeking financial damages and a permanent injunction that would shut down Corellium's iOS virtualization service.

Corellium warns customers about infringement

We contacted Corellium about Apple's lawsuit today and will update this story if we get a response. Corellium is based in Florida. Its website doesn't let potential customers purchase access to virtual machines directly. Instead, it provides an email address for contacting Corellium's sales department.

Corellium's intellectual property policy says the company "respects the Intellectual Property rights of others," and that it terminates the accounts of Corellium customers "who infringe or are repeatedly charged with infringing the Intellectual Property rights of others." The company also says that customers may not "make any copies" of Corellium's software or "resell, distribute, or sublicense" the Corellium Software. But the intellectual property policy doesn't explain how Corellium selling access to copies of iOS complies with Apple's copyrights.

Corellium says it indemnifies its customers against claims

that Corellium’s software infringes other companies’ intellectual property rights.

https://arstechnica.com/?p=1552897

Judge orders Georgia to switch to paper ballots for 2020 elections

Enlarge / An election official holds an electronic voting machine memory card following the Georgia primary runoff elections at a polling location in Atlanta, Georgia, US, on Tuesday, July 24, 2018.
Elijah Nouvelage/Bloomberg via Getty Images

reader comments

181 with 102 posters participating, including story author

Share this story

Election security advocates scored a major victory on Thursday as a federal judge issued a 153-page ruling ordering Georgia officials to stop using its outdated electronic voting machines by the end of the year. The judge accepted the state’s argument that it would be too disruptive to switch to paper ballots for municipal elections being held in November 2019. But she refused to extend that logic into 2020, concluding that the state had plenty of time to phase out its outdated touchscreen machines before then.

The state of Georgia was already planning to phase out its ancient touchscreen electronic voting machines in favor of a new system based on ballot-marking machines. Georgia hopes to have the new machines in place in time for a presidential primary election in March 2020. In principle, that switch should address many of the critics' concerns.

The danger, security advocates said, was that the schedule could slip and Georgia could then fall back on its old, insecure electronic machines in the March primary and possibly in the November 2020 general election as well. The new ruling by Judge Amy Totenberg slams the door shut on that possibility. If Georgia isn't able to switch to its new high-tech system, it will be required to fall back on a low-tech system of paper ballots rather than continue using the insecure and buggy machines it has used for well over a decade.

Alex Halderman, a University of Michigan computer scientist who served as the plaintiffs' star witness in the case, hailed the judge's ruling.

"The court's ruling recognizes that Georgia's voting machines are so insecure, they're unconstitutional," Halderman said in an email to Ars. "That's a huge win for election security that will reverberate across other states that have equally vulnerable systems."

Georgia's voting technology is deeply flawed

Totenberg's ruling is 153 pages long because it presents a mountain of evidence that Georgia's touchscreen voting machines—as well as back-office software the state uses to manage voter registrations, design ballots, and count votes—are outdated and insecure.

Georgia is still using Diebold Accuvote TSX touchscreen machines whose hardware and software date back to around 2005. In 2006 and 2007, security researchers discovered numerous security vulnerabilities in these machines—problems serious enough to cause California to decertify them from use in state elections.

After one 2006 report, Totenberg writes, "Diebold was forced to create a security patch for the vulnerable TSX software." Yet incredibly, "there is no evidence that Georgia ever implemented the software patch or made any upgrades to protect the integrity of its DRE machines," Totenberg says.

The security problems found by those early researchers were serious. Not only can someone with physical access to the machine install vote-stealing malware, it's also possible to deliver such malware using viruses that spread from machine to machine on the memory cards election workers use to load ballot information onto them. Hence, a malicious actor with a few minutes' access to a single machine could potentially hack dozens or even hundreds of machines.

These concerns seemed somewhat theoretical when they were first raised around 2006. After all, who would want to hack an election? But they've been given added urgency after revelations that the Russian government actively probed state election systems—including in Georgia—in 2016.

Not actually air-gapped

Besides hacking voting machines directly, another way someone could compromise an election would be to first hack the office computers of election officials. Officials use these computers to create ballot definition files that are later transferred to voting machines via memory cards. Here too, there's a risk that malware could ride along with the ballot files and infect machines.

Georgia election officials dismissed these concerns. In 2018 testimony before Judge Totenberg, official Michael Barnes insisted that the computers used to design electronic ballots were air-gapped from the Internet, making it impossible for remote attackers to compromise them. But subsequent testimony made it clear that this was wrong. In reality, Totenberg writes, ballots were designed "on public-facing internet-connected desktop computers of the individual ballot builders, then copied over from the public facing computer onto a 'lockable' USB drive for transfer to the 'air-gapped' system."

In court testimony, Halderman pointed out that this setup isn't actually secure. "Air-gapping" a computer does no good if people are regularly transferring files to it from Internet-connected computers.

It gets worse. In 2016, a Georgia-based security researcher discovered that Kennesaw State University's Center for Election Systems, which has a contract to help Georgia manage its elections, had a massive cache of sensitive election-related documents—including private voter data and passwords for election systems—publicly available on its website for anyone to download. After being notified of the breach, it took officials months to remove the sensitive information from the website.

Many voters reported problems with the machines

Meanwhile, dozens of ordinary Georgia voters told the court that they had experienced problems with Georgia's touchscreen machines. Totenberg describes one voter's experience:

> *Teri Adams described that when she voted at the Bleckley County Courthouse and selected candidate Stacey Abrams for governor on the DRE screen, she noticed that her designated selection was listed as Brian Kemp on the review screen. She*

> *tried to vote for Abrams a second time, but the review screen again showed Kemp as her chosen candidate. Ms. Adams cast her ballot on the third try when her selection in the governor's race remained Abrams. Adams reported her problems on "machine number 2" to the poll workers whose only response was "did it take your vote?"*

Adams was hardly an isolated case. A number of voters reported that it took two or three tries to ensure that a voting machine was choosing their preferred candidate.

Is this evidence that hackers were tampering with the election? Probably not. It seems more likely that Georgia's touchscreen machines are just old and poorly designed. Someone who hacked the machines in order to steal the election wouldn't have any reason to alarm voters by showing the stolen vote on the screen—they could show the voter's correct choice on the screen while recording a different result in the electronic record.

But the fact that so many voters have reported problems with the machines is a problem in its own right. A mis-recorded vote is a problem regardless of whether it was the result of hacking, malfunctioning equipment or just a badly designed user interface. And there's now ample evidence that touchscreen machines are a less effective way to record voters' choices than a traditional paper ballot.

Georgia must stop using its machines after 2019

Judge Totenberg had all of these problems in mind as she was deciding what to do with the lawsuit. She was convinced by the plaintiffs' argument that Georgia's current election system was fatally flawed and needed to be overhauled—and that a hand-marked paper ballot was the gold standard for secure and

reliable voting.

At the same time, she took seriously warnings from the state of Georgia that an abrupt shift to paper ballots could cause more disruption than it was worth. The issue was complicated by the fact that Georgia's legislature recently passed legislation directing that the state develop a new election system based on ballot-marking devices—electronic voting machines that print out a paper ballot the voter can examine.

Georgia has signed a contract with a vendor for these new machines and plans to start testing them in a few cities in this November's elections. The state aims to start rolling the new system out statewide in time for next March's presidential primary. Under that timeline, the state would stop using its current, insecure machines before the end of the year.

The problem, critics point out, is that the state may not be able to roll out the new system in time for next March's election. Experts testified that Georgia has set an unusually aggressive timeline for standing up a completely new election system, and this creates a risk that the schedule could slip. In that case, Georgia's most likely fallback would be to continue using its existing touchscreen machines for the spring primary election—and possibly even the November 2020 general election.

So Judge Totenberg decided to split the difference. She denied the plaintiffs' request to force Georgia to begin using paper ballots in the November 2019 election. She accepted the state's argument that it would be a waste of resources to set up a paper-based system that will only be used in a single election—and that such an order could distract from efforts to develop the new system for 2020.

However, she also ordered the state not to use its old touchscreen machines as a fallback for elections in 2020. If the new ballot-marking devices aren't ready by March, the

state will be required to use hand-marked paper ballots instead.

People are finally listening to computer scientists

The order is an important ruling for voters in Georgia, who won't have to worry about outdated equipment failing to accurately record their vote in 2020. But the ruling is also an important milestone in the broader debate over voting machine security. Judge Totenberg's ruling is a strong endorsement of the consensus of computer security experts about the dangers of computer-based voting. Princeton computer scientist Andrew Appel put it well in a report quoted by Totenberg:

> *All digital information—such as ballot definitions, voter choice records, vote tallies, or voter registration lists—is subject to malicious alteration; there is no technical mechanism currently available that can ensure that a computer application—such as one used to record or count votes—will produce accurate results; testing alone cannot ensure that systems have not been compromised; and any computer system used for elections—such as a voting machine or e-pollbook—can be rendered inoperable.*

As a result of these arguments, most computer scientists favor voting via a hand-marked paper ballot. They believe that computerized optical scanners are a reasonable way to speed up the vote-counting process provided that a state also provides for routine post-election audits that hand count a random sample of ballots to verify the accuracy of the machine count.

Federal legislation to strengthen election security has been blocked by Senate Majority Leader Mitch McConnell. But that doesn't preclude changes at the state level, with the courts

spurring states along in the most egregious cases. Totenberg's clear and thorough ruling will give opponents of electronic voting machines a bit of extra momentum as they race to decommission as many electronic voting machines as possible before the November 2020 presidential election.

https://arstechnica.com/?p=1552423

Disney fights streaming account sharing with help from cable industry

Enlarge / Here they come, all together in a streaming bundle.
Disney / Sam Machkovech

reader comments

158 with 115 posters participating

Share this story

Ars Guide to Online Security

View more stories

Disney and Charter Communications are teaming up to fight account sharing in an attempt to prevent multiple people from using a single account to access streaming video services.

The battle against account sharing was announced as Disney and the nation’s second-biggest cable company struck a new distribution agreement involving Disney’s Hulu, ESPN+, and the forthcoming Disney+. Customers could still buy those online services directly from Disney, but the new deal would also let them make those purchases through Charter’s Spectrum TV service.

If you buy a Disney service through Charter, be aware that the companies will work together to prevent you from sharing a login with friends. Disney and Charter said in their announcement yesterday that they have “agreed to work together on piracy mitigation. The two companies will work together to implement business rules and techniques to address such issues as unauthorized access and password sharing.”

In addition to streaming services, the deal will let Charter continue carrying Disney-owned TV channels on its cable service. That includes ABC, the various Disney and ESPN channels, FX, National Geographic, and more.

“This agreement will allow Spectrum to continue delivering to its customers popular Disney content, makes possible future distribution by Spectrum of Disney streaming services, and will begin an important collaborative effort to address the significant issue of piracy mitigation,” Charter Executive VP Tom Montemagno said.

The announcement didn’t say exactly how the companies will fight account sharing. We asked Charter for technical details on how it’ll work and about whether this will result in more personal customer data being shared between Charter and Disney. Charter did not answer any of our questions, saying, “we don’t have details to share at this time.”

We sent the same questions to Disney and will update this article if we get any answers.

Charter CEO complained about account sharing

The crackdown could target people who use Charter TV account logins to sign into Disney services online. Charter CEO Tom Rutledge has complained about account sharing several times over the past few years while criticizing TV networks for not fully locking down their content.

“There’s lots of extra streams, there’s lots of extra passwords, there’s lots of people who could get free service,” Rutledge said at an industry conference in 2017. He argues that password sharing has helped people avoid buying cable TV. ESPN has also complained about account sharing, calling it piracy.

Another possibility is that Charter could monitor usage of its broadband network to help Disney fight account sharing. For example, Disney could track the IP addresses of users signing in to its services, and Charter could match those IP addresses to those of its broadband customers. Charter has plenty of leeway to share its customers’ private browsing data because the Republican-controlled Congress eliminated broadband privacy rules in 2017.

Customers could use VPN services to attempt to avoid detection, though.

Charter has 15.8 million residential TV customers nationwide, making it the second-biggest cable TV service after Comcast. But it lost 400,000 video customers in the past year. Charter’s broadband service has gone in the other direction, rising from 23.1 million to 24.2 million residential customers in the past year.

Netflix and HBO take less strict approach

In contrast to Charter and Disney, Netflix and HBO haven't cared as much about account sharing.

Sharing a Netflix account "with individuals beyond your household" does violate Netflix's terms of use, but the restriction isn't heavily enforced. "Password sharing is something you have to learn to live with, because there's so much legitimate password sharing, like you sharing with your spouse, with your kids," Netflix CEO Reed Hastings said in 2016.

Now-former HBO CEO Richard Plepler once said that password sharing is a "terrific marketing vehicle for the next generation of viewers" and that "we're in the business of creating addicts." (Plepler left HBO in February, less than a year after AT&T bought HBO owner Time Warner.)

Netflix, HBO, and the Disney-owned Hulu all limit the number of concurrent streams on each account, however. That doesn't prevent account sharing entirely, but such a policy can make it inconvenient to share an account with a bunch of friends.

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

https://arstechnica.com/?p=1552355

Woman accused of Capital One hack had stolen data from 30 companies, authorities say

Enlarge / Paige Thompson, 33, a former Seattle technology company software engineer, was arrested after she boasted about a massive data theft from Capital One on GitHub. She is now accused of 30 other data thefts.

reader comments

59 with 38 posters participating

Share this story

In a petition filed on August 13 in federal court in Seattle, the Justice Department asserted that Paige Thompson—the former Amazon employee accused of stealing data from Capital One credit card applications—had done far more, including "major cyber intrusions that resulted in the theft of massive amounts of data from what now appears to be more than 30 victim companies." US Attorney for Western Washington Brian Moran's filing was for a motion to keep Thompson imprisoned until trial because she is a flight risk and "has a long history of threatening behavior that includes repeated threats to kill others, to kill herself, and to commit suicide by cop."

Aside from Capital One, the victim organizations have not been named by Justice officials, but the filing stated that they included "other companies, educational institutions, and other entities." The data from these sources reviewed thus far appears largely to not include personal information.

"At this point, however, the government is continuing to work

to identify specific entities from which data was stolen, as well as the type of data stolen from each entity," Moran wrote in his filing. "The government expects to add an additional charge against Thompson based upon each such theft of data, as the victims are identified and notified."

Thompson is not believed to have sold or shared any of the data she stole or profited from it in any way. The copy of the data recovered by law enforcement during the search of Thompson's home "is the only copy of the stolen data that she created," the filing states, but "it is too early to confirm that this is the case…the government is continuing its investigation, which will take a significant amount of time and resources, given the immense amount of forensic evidence to review."

Thompson, who called herself "erratic" online, "appears to have significant mental-health issues," and she would be a threat to others and herself if released, Moran's filing explained. Thompson said in a direct message thread on Twitter that she was "ready to check the fuck out" and that she "prefer[red] to die, and something to make it easy." She also threatened to kill police in a Twitter post, as well as the person who called them.

- A threatening Twitter post from Thompson .
- "Ready to check out."

In 2018, two people filed for protection orders against Thompson. And police had been called to Thompson's home twice in 2019. In March, she "became violent with her housemates" and then threatened to use a fake gun to commit "suicide by cop" when the police were called. In May, Moran stated, "police were called to Thompson's residence after Thompson contacted an acquaintance at a California technology office and threatened to travel to the company's campus in California and to 'shoot up' the office." One of Thompson's roommates had

a collection of assault rifles, Moran said.

https://arstechnica.com/?p=1551769