Breach affecting 1 million was caught only after hacker maxed out target’s storage



reader comments

36 with 24 posters participating

Share this story

The US Federal Trade Commission has sued an IT provider for failing to detect 20 hacking intrusions over a 22-month period, allowing the hacker to access the data for 1 million consumers. The provider only discovered the breach when the hacker maxed out the provider’s storage system.

Utah-based InfoTrax Systems was first breached in May 2014, when a hacker exploited vulnerabilities in the company’s

network that gave remote control over its server, FTC lawyers alleged in a complaint. According to the complaint, the hacker used that control to access the system undetected 17 times over the next 21 months. Then on March 2, 2016, the intruder accessed personal information for about 1 million consumers. The data included full names, social security numbers, physical addresses, email addresses, phone numbers, and usernames and passwords for accounts on the InfoTrax service.

The intruder accessed the site later that day and again on March 6, stealing 4,100 usernames, passwords stored in clear-text, and hundreds of names, addresses, social security numbers, and data for payment cards.

The complaint said InfoTrax employees did not discover the breach until March 7, 2016, when they received alerts that one of the company's servers had reached its maximum storage capacity. The alert was the result of the intruder creating a data archive file that had grown so large that a hard drive ran out of space. It was only then, FTC attorneys said, that InfoTrax began taking steps to secure its network.

Even after the breach came to light, the InfoTrax network was compromised at least two more times, the FTC alleged. One week later, an intruder used malicious code to collect data through an InfoTrax customer's website that harvested more than 2,300 unique, full payment card numbers, including names, physical addresses, CVVs, and expiration dates. Then on March 29, an intruder used the user ID and password of an InfoTrax client to upload more malicious code. The intruder used the access to collect newly submitted payment card data.

InfoTrax's "failure to provide reasonable security for the personal information of distributors and end consumers has caused or is likely to cause substantial injury to consumers in the form of fraud, identity theft, monetary loss, and time spent remedying the problem," FTC lawyers wrote in the complaint. They said a call center retained by one InfoTrax

client seeking help with the breach response received more than 238 complaints of unauthorized payment card charges, 34 complaints of new credit lines opened, 15 complaints of tax fraud, and one complaint of misuse of information for employment purposes.

Specific failures alleged by the FTC against InfoTrax included not:

- taking inventory and deleting personal data it no longer needed
- conducting code review of its software and testing the security of its network
- detecting malicious file uploads
- adequately segmenting its network
- implementing security safeguards to detect suspicious activity on its network

The FTC said in a statement that as part of a proposed settlement, InfoTrax will be barred from collecting, selling, sharing, or storing personal information unless the company implements a security program that corrects the failures identified in the complaint. InfoTrax will also be required to obtain third-party assessments of its security every two years.

https://arstechnica.com/?p=1601719

How the FCC solves consumer problems—well, it doesn’t,

really



Enlarge / FCC Chairman Ajit Pai.

reader comments

117 with 64 posters participating

Share this story

The Federal Communications Commission’s extremely hands-off approach to broadband-customer complaints has alarmed a member of Congress.

US Rep. Mike Quigley (D-Ill.) wrote a letter to FCC Chairman Ajit Pai in August after learning of a Frontier customer who was forced to pay a $10-per-month rental fee for a router despite buying his own router.

As we wrote at the time, Frontier charges customers a $10 monthly fee for routers even when the company doesn’t provide

one at all, saying that non-Frontier routers cause “increased complaints and more difficulty with troubleshooting.” But Frontier *also* said it “cannot support or repair the non-Frontier equipment,” so it’s charging $10 a month without providing a router or providing support for non-Frontier routers.

The case we wrote about was particularly egregious, because the customer was using a FiOS router he had purchased from Verizon before Verizon sold its network in Texas to Frontier. The router was specifically designed to work with Frontier’s FiOS service and the customer owned it outright, but he still had to pay an extra $10 a month.

The customer, Rich Son, filed a complaint to the FCC. Frontier responded by insisting that it must continue charging the fee, and the FCC then told Son that “We believe your provider has responded to your concerns.”

So what does complaining to the FCC actually accomplish, especially after the FCC’s December 2017 vote to deregulate the broadband industry in its “Restoring Internet Freedom” order? That’s what Rep. Quigley wanted to find out. After hearing the FCC’s response to his questions, the lawmaker was disappointed and told Ars that Pai has “abdicated” his responsibility over broadband.

What does the FCC do?

Quigley is one of numerous Democrats who have expressed concern about the FCC giving up its Title II authority to regulate broadband. Pai has repeatedly passed the buck to the Federal Trade Commission on enforcement, but the FTC has to regulate many industries, leaving it little time for broadband. Pai leads what is supposed to be the government’s top agency for telecom regulation, but he has done little to help consumers in billing disputes that are specific to telecom services.

“Frontier’s justifications are difficult to follow,” Quigley wrote in his letter to Pai. “Routers are common equipment, and millions of Americans use their own devices to access broadband and television communications services. Ample troubleshooting resources exist online. I find it difficult to see how this fee serves as anything other than a way for Frontier to disguise the true cost of its service to customers.”

Frontier’s policy also “undercuts long-standing, hard-fought precedent that consumers should be able to use their own devices with communications networks,” and “reveals just how harmful the Commission’s Restoring Internet Freedom order has been to Americans,” he wrote.

Quigley’s letter went on ask a series of questions about whether the FCC still has jurisdiction over broadband-and-cable-TV billing disputes and how it handles customer complaints. It said, in part:

> *How many complaints has the FCC received about broadband equipment rental fees in the past year? Has it conducted an analysis of any of these complaints? If so, what did the FCC find? If not, why not? How did the FCC respond to these complaints? Does the FCC plan to make a substantive response to these types of complaints?*

Quigley also noted that the FCC pledged to work closely with the FTC on consumer complaints in a December 2017 Memorandum of Understanding in which the agencies said they would discuss potential investigations, coordinate investigatory activities, and share consumer complaints. Given that, Quigley asked Pai how many complaints his agency has referred to the FTC, whether the FCC monitors the progress of those complaints, and whether the FCC has assisted the FTC in any investigations into broadband-billing practices.

Pai’s response

It turns out that the FCC hasn’t proactively forwarded any broadband-billing complaints to the FTC despite the agencies’ working agreement. But Pai’s initial response to Quigley didn’t reveal that tidbit.

Pai’s response letter told Quigley that consumers filed 450 informal complaints about broadband-equipment rental fees in the past year and that “nearly all” of them were “served on the relevant provider for a response.”

Pai’s letter also said that complaints about “unfair or deceptive billing practices by Internet service providers have been referred to the FTC.” What isn’t clear from that statement is how many complaints were forwarded to the FTC and under what circumstances the FCC decides to forward them. Pai also told Quigley that the FCC doesn’t have any information about what happened to those complaints after they were sent to the FTC.

After the exchange of letters, Quigley’s staff followed up with the FCC to find out how the agency decides whether to forward complaints to the FTC. The answer from FCC staff was that it hasn’t forwarded any billing complaints to the FTC without being asked to do so first, Quigley’s staff told Ars. The FCC apparently only forwarded complaints to the FTC when the FTC asked for a set of complaints about particular companies.

“At no point has the FCC actually sent, of their own volition, a single complaint to FTC for enforcement,” a Quigley senior staff member told Ars. “So essentially what the FCC is saying is, ‘If you complain to us, we have to send a letter [to your ISP] that recognizes that we got a complaint within 30 days. And if we do that, that’s the extent of our responsibility.’ Now, the second part of that is, [the FCC says that] ‘If we think it’s a really big deal and should rise to the level of

enforcement, we'll send it to the FTC.' But [the FCC has] never done that."

The FCC told Quigley's office that, since the Restoring Internet Freedom order, it has referred 4,228 broadband-billing complaints to the FTC but that all of those were specifically requested by the FTC. The FTC asked for those complaints in one case "related to an AT&T unauthorized cellular data plan" and in another "related to a Frontier Internet speed issue," the Quigley staff member told Ars.

Committee staff was "floored" by response

We contacted Pai's office yesterday morning to confirm this and haven't gotten a response. We contacted the FTC about the investigations into AT&T and Frontier today, and a spokesperson told us the FTC doesn't comment on whether it is investigating any particular company or practice.

"Somehow, the FCC has not received a single complaint that they think requires enforcement action or any followup whatsoever, beyond the recognition that they received this complaint," the Quigley staff member told Ars. "When our committee staff heard about this, they were floored. This is certainly not what the FCC initially implied when they responded to our inquiry, and it's pretty alarming."

Quigley, who is chairman of the Financial Services and General Government (FSGG) subcommittee, sent Ars the following statement:

> *As the agency with the most expertise in communications, the FCC should ensure the American people don't fall victim to abusive business practices. Instead, Chairman Pai has abdicated responsibility over broadband services entirely to another agency. I am deeply dismayed that the FCC seems to*

> *have washed its hands of consumer protection in this area and has simultaneously fallen woefully short of providing Americans with their knowledge and expertise. As Chairman of the FSGG subcommittee, I am committed to ensuring that agencies like the FCC prioritize people over corporate profit and live up to the expectations of Congress and the American people.*

Quigley is busy with Trump impeachment proceedings right now because he also serves on the House Intelligence Committee, but his staff told us that he'll take action on the FCC matter later. That will likely include more extensive questioning of Pai at future FCC budget hearings and possibly legislation.

https://arstechnica.com/?p=1601515

Google will offer checking accounts, says it won't sell the data



Enlarge / Google logo seen during Google Developer Days (GDD) in Shanghai, China, September 2019.

reader comments

146 with 108 posters participating

Share this story

The Google empire is enormous and ubiquitous, covering basically the entire Internet in one way or another. There is, however, one lucrative business the company does not yet have a foothold in: banking. And now it has plans to change that.

Google is working to launch consumer checking accounts next year, The Wall Street Journal first reported this morning. The project, code-named Cache because apparently nobody can resist a pun, is expected to launch next year, sources told the Journal. CNBC, also citing “sources familiar,” confirmed the WSJ’s reporting.

Google: Not a bank

The accounts will be run in partnership with Citibank and a credit union based out of Stanford University. Google executive Caesar Sengupta told the WSJ that the accounts will carry branding from the banks, not from Google, which will also “leave the financial plumbing and compliance” to the banks.

Google and its partners are still hammering out the details of these accounts, including whether or when accounts might incur fees. (Many banks that offer checking accounts waive monthly fees for customers who maintain a certain average balance or who use direct deposit.)

“Our approach is going to be to partner deeply with banks and the financial system,” Sengupta told the WSJ. “It may be the slightly longer path, but it’s more sustainable.”

Banks are subject to fairly strict regulatory standards. An institution offering a checking account must comply with a lengthy list of federal laws, as well as any relevant state laws that might apply.

That’s the same kind of partnership Google’s major mobile competitor Apple has taken. Apple this summer launched a credit card that all US iPhone users are eligible to apply for. While the card carries Apple branding and is managed through an Apple-designed iPhone app, the bank behind the card is Goldman Sachs, which took the partnership as an opportunity to expand its individual consumer business.

A partnership with Google could be a similar opportunity for Citibank. Citi is the nation’s third-largest bank, behind JPMorgan Chase and Bank of America, but has a smaller retail banking footprint. Chase operates about 5,000 US branches, and CEO Jamie Dimon said earlier this year it plans to cover about 93% of the US population by 2022. BoA has about 4,300 branches

and says its footprint will encompass 90% of the United States by 2021. Citi, on the other hand, operates about 700 branches and has about $800 billion less in assets than Chase does.

For Google's part, there are two populations such an arrangement could easily zero in on, without even doing any work to convince current checking-account holders to switch. First: younger consumers. Teenagers and young adults are digital natives, already using their phones for everything, but they may not yet have settled in with a bank anywhere yet. Any of those who have Android phones could be an easy built-in market.

Second: the un- and underbanked, who are not currently served well by traditional financial institutions. About 6.5% of US households were completely unbanked in 2017, according to federal data, and another 18.7% were underbanked. That population, about 33 million households, skews heavily toward low- and very low-income individuals—groups who are likely to use inexpensive Android phones as their main method of connecting to the Internet.

The data machine

If you want to know almost everything about a person, you can look at their bank account. Your pay goes in, with a very precise amount and source, and your spending—where, when, how, and how much—all comes out.

Google wants to "bring value to consumers, banks, and merchants, with services that could include loyalty programs," the WSJ reports, but Sengupta said the business does not intend to sell checking-account customers' financial data. The company also told the WSJ that it does not use data from Google Pay for advertising purposes or share that data with advertisers.

That's a choice that Google could easily change, however.

There are very clear regulations about what data banks can share about you, but those policies end up saying they can share quite a lot of information, and you can’t limit most of that sharing. Regulation has largely not yet caught up to mobile wallets such as Google Pay and Apple Pay, meanwhile, so those exist in something of a gray space.

In 2014, during the Obama administration, the Consumer Financial Protection Bureau began examining the implications of mobile payment services, including issues relating to data and privacy. CFPB action has been curtailed during the Trump administration, however, with current director Kathy Kraninger significantly cutting back on bureau activity and agreeing the agency is unconstitutional.

But unspecified advertisers outside of Google are not the only concern. The company is large enough, with enough enterprises under its umbrella, for users to have legitimate concern about data use by Google, inside Google.

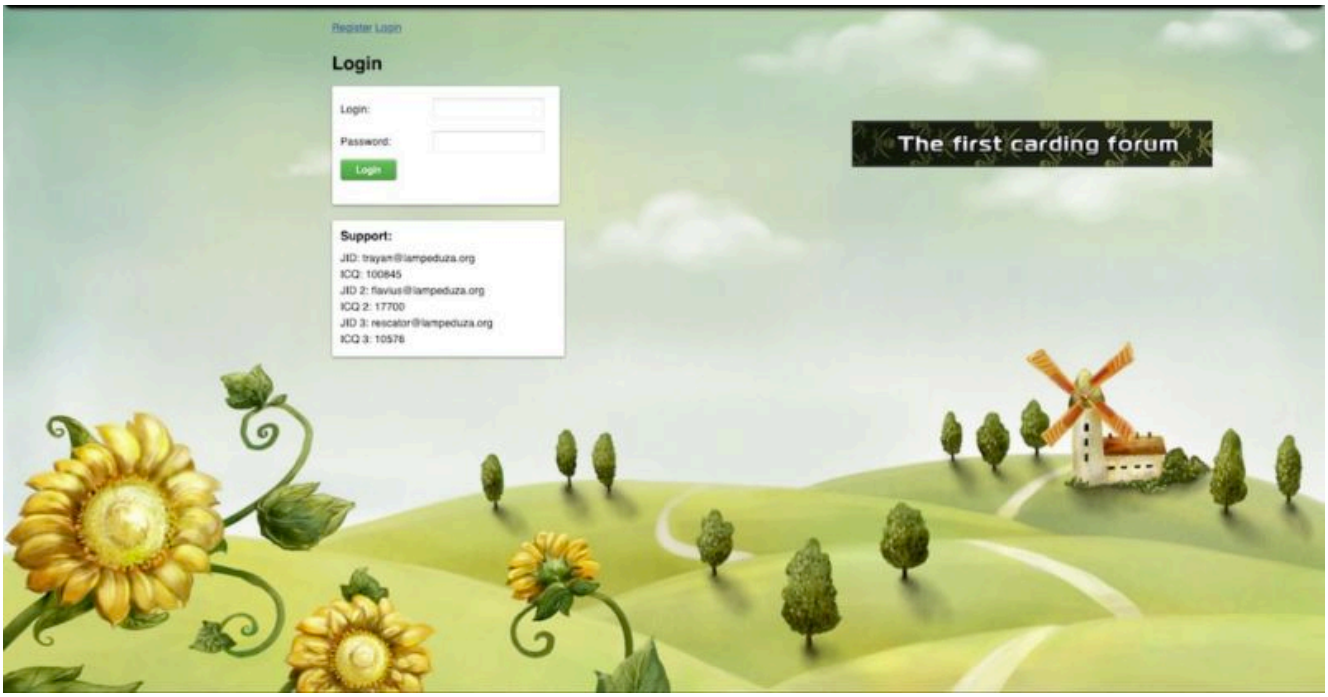
Earlier this week, The Wall Street Journal reported that Google is hoovering up health care data from tens of millions of patients, potentially adding fuel to the criticisms that the company is too big and has far too much user data accumulated.

Sen. Mark Warner (D-Va.) told CNBC today he has concerns about the proposal.

“We’re going to see greater use of data in all sectors, including finance” Warner said. “I’m concerned, whether it’s [Facebook’s] Libra or whether it’s the Google proposal around banking, where we have these giant tech platforms entering into new fields before there are some regulatory rules of the road. Because once they get in, the ability to extract them out is going to be virtually impossible.”

https://arstechnica.com/?p=1601395

Russian man charged with running money-back-guaranteed criminal marketplace



Enlarge / The front page of cardplanet.cc as it appeared on August 1, 2015.

reader comments

30 with 27 posters participating

Share this story

A Russian man made his initial appearance in federal court on Tuesday on prosecutors' allegations he operated websites that resulted in more than $20 million in fraudulent purchases made on US credit cards.

Aleksei Burkov, 29, of Tyumen and St. Petersburg, Russia, arrived at Dulles International Airport on Monday night after

he was arrested in Israel in late 2015, federal prosecutors said. His extradition came after appeals to the Israeli Supreme Court and the Israeli High Court of Justice were denied. Tuesday's appearance was before the US District Court for the Eastern District of Virginia.

According to an indictment that was unsealed on Tuesday, Burkov ran a website, called Cardplanet, that sold card data for anywhere from $2.50 to $60 apiece, depending on the card type, country of origin, and the availability of the cardholder's name, address, and other identifying information. In all, Cardplanet offered for sale more than 150,000 compromised payment cards, including "at least tens of thousands" of which had been issued to holders located in the US.

In August 2015—four months before Burkov was arrested at Israel's Ben-Gurion Airport near Tel Aviv—the site's front page provided a simple login box along with support contacts and artwork, according to the Internet Archive. Prosecutors said Burkov advertised Cardplanet as "the only service that would refund the price of invalid card data." The site allegedly offered a fee-based service called Checker, which allowed customers to instantly verify if stolen payment cards were still valid.

Burkov allegedly ran a second site that allowed criminal hackers to advertise the sale of personal identity information, malware, and illegal services. The site operated on an invitation-only basis. To be admitted, candidates had to be vouched for by three existing members and pay a $5,000 entrance fee as insurance. The admittance rules were designed to thwart law enforcement investigators and to ensure that members honored any deals they made on the forum.

Burkov is charged with wire fraud, access device fraud, and conspiracy to commit wire fraud, access device fraud, computer intrusions, identity theft, and money laundering. If convicted

on all counts, he faces a maximum of 80 years in prison, although actual sentences are typically less than the maximum. Prosecutors are also seeking the forfeiture of more than $21 million in US currency and any other proceeds resulting from the alleged crimes.

It’s not clear when an arraignment is scheduled or if Burkov has been assigned an attorney.

https://arstechnica.com/?p=1601205

EPA still moving to limit science used to support regulations



Enlarge / Environmental Protection Agency Administrator Andrew Wheeler.

reader comments

49 with 35 posters participating

Share this story

Former Texas Congressman Lamar Smith may have retired in January, but his ideas still stalk the halls of the US Environmental Protection Agency. The New York Times reported Monday that the latest incarnation of Smith's quest to change the science the EPA can use for its rule making is moving forward.

Smith had unsuccessfully pushed a bill called the "Secret Science Reform Act," which would have required the EPA to consider only those studies with data that is "publicly available in a manner sufficient for independent analysis and substantial reproduction of research results." He claimed that

opponents of regulations were often unable to audit the science underlying the regulations—although those opponents could, of course, have done their own science.

Limiting science

The scientific community noted that this requirement would have the effect of excluding quite a lot of relevant science published in peer-reviewed journals. In particular, research on the public health impacts of pollutants is only possible through the use of confidential health data. There are systems in place to give researchers controlled access to that data, but releasing it to the public is simply not an option, and doing so very well might violate other federal rules.

Smith couldn't get his bill through Congress, but he worked with former EPA Administrator Scott Pruitt to get it rolling as an internal agency rule change. A 2018 E&E News story reported that this collaboration ran into an unlikely opponent: the pesticide industry. Those companies must provide safety studies when registering a new pesticide, so they were concerned about the cost of making all their data publicly available, and they were unclear on what form that would take.

The rule change was not finalized before Pruitt's resignation, and current EPA Administrator Andrew Wheeler appeared to take it back to the drawing board. But in a surprising twist, a new draft has appeared that The New York Times described as "headed for White House review." The twist is that the new draft doesn't do much to refocus the rule in a more narrow way that minimizes industry objections. Instead, it has been made broader in some ways.

The first version of the rule only covered the research that quantifies toxicity of things like pollutants and pesticides. This draft removes that limitation. "EPA is modifying the regulatory text initially proposed in the 2018 proposed Rule[…]" it reads, "so that these provisions would apply to

all data and models, not only dose-response data and dose-response models."

Retroactive

What's more, the rule isn't just for new studies—it could end up applying retroactively. The draft contains multiple options on a couple points, one of which is setting a date *after* which research would have to comply with these requirements. But if that isn't the option chosen, it would mean that all past research for which data has not been made publicly available would be found to fail the test. If a regulation comes up for renewal or updating, the science on which it was based could then plausibly be excluded from consideration.

Options are also listed for the issue at the heart of the rule—what to do with data that isn't sufficiently public. There are two alternatives to simply dropping that data in the trash bin. One would be to make availability part of the *weighting* of a study's value. This might not immediately disqualify a study if other characteristics of the work are seen as redeeming. However, the draft reads, "EPA would reserve the right to place less weight on the studies, to the point of entirely disregarding them, if the data and models underlying pivotal regulatory science are not made available in full to EPA."

The other alternative would recognize several tiers of data, from publicly available to "confidential business information" to "personally identifiable information that cannot be anonymized." Access would be different for each tier, with proprietary or personal information only required to be available to "authorized officials and researchers" rather than the general public. It's not clear how many privacy problems that would solve, although it would be easier for companies to navigate, as they would only have to respond to requests rather than publishing their data somewhere

permanent.

Assuming this draft goes forward, it will once again be opened to public comment. When Pruitt's version went to public comment last year, more than 590,000 such comments were submitted.

https://arstechnica.com/?p=1600865

US violated Constitution by searching phones for no good reason, judge rules



Enlarge / US Customs and Border Protection agents participate in a training exercise at a vehicle entry point along the

border with Mexico on November 5, 2018, in Hidalgo, Texas.

reader comments

69 with 55 posters participating

Share this story

The United States government violated the Fourth Amendment with its suspicionless searches of international travelers' phones and laptops, a federal court ruled today.

The ruling came in a case filed "on behalf of 11 travelers whose smartphones and laptops were searched without individualized suspicion at US ports of entry," the American Civil Liberties Union (ACLU) said today. The ACLU teamed up with the Electronic Frontier Foundation (EFF) to fight the government on behalf of plaintiffs including 10 US citizens and one lawful permanent resident.

The order from a US District Court in Massachusetts limits what searches can be made by US Customs and Border Protection (CBP) and US Immigration and Customs Enforcement (ICE).

"The district court order puts an end to CBP and ICE's asserted authority to search and seize travelers' devices for purposes far afield from the enforcement of immigration and customs laws," the ACLU announcement said. "Border officers must now demonstrate individualized suspicion of contraband before they can search a traveler's device."

Because of the ruling, travelers will be able to "cross the international border without fear that the government will, in the absence of any suspicion, ransack the extraordinarily sensitive information we all carry in our electronic devices," EFF Senior Staff Attorney Sophia Cope said.

The US government could appeal the ruling.

Judge: Searches require reasonable suspicion

US District Judge Denise Casper's ruling granted the plaintiffs' request for a declaration that the government violated their constitutional rights by conducting searches and seizures "of electronic devices absent a warrant supported by probable cause."

The ruling said:

> *[T]he Court declares that the CBP and ICE policies for "basic" and "advanced" searches, as presently defined, violate the Fourth Amendment to the extent that the policies do not require reasonable suspicion that the devices contain contraband for both such classes of non-cursory searches and/or seizure of electronic devices; and that the non-cursory searches and/or seizures of plaintiffs' electronic devices, without such reasonable suspicion, violated the Fourth Amendment.*

CBP defines "advanced" searches as those "in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents." Anything short of that is a "basic" search.

The court ruling said that CBP's policy was "to require reasonable suspicion or a national security concern for any advanced search, but no showing of cause for a basic search." The judge ruled that both types of searches require reasonable suspicion.

"Although governmental interests are paramount at the border, where such non-cursory searches—even 'basic' searches as broadly defined under CBP and ICE policies as well as the 'advanced' searches of plaintiffs' electronic devices—amount

to non-routine searches, they require reasonable suspicion that the devices contain contraband," Casper wrote.

It wasn't all good news for plaintiffs though: Judge Casper's ruling denied their request for an injunction that would have more strictly limited the government's ability to search and seize devices. But the ruling denied the request for injunctive relief *without prejudice*, so it can be raised again in future proceedings. To apply a nationwide injunction, the court would need "further briefing from the parties" involved in the case, Casper wrote.

Despite that, the ACLU said the ruling should lead to real change in government policy.

"This ruling significantly advances Fourth Amendment protections for the millions of international travelers who enter the United States every year," ACLU staff attorney Esha Bhandari said. "By putting an end to the government's ability to conduct suspicionless fishing expeditions, the court reaffirms that the border is not a lawless place and that we don't lose our privacy rights when we travel."

Some plaintiffs' phones were searched repeatedly

Casper's ruling contains some details of the contested searches and seizures. Nadia Alasaad, one of the 11 plaintiffs, "has twice had her iPhones searched at the border over her religious objections to having CBP officers, especially male officers, view photos of her and her daughters without their headscarves as required in public by their religious beliefs," the ruling said.

One plaintiff "observed a CBP officer viewing communications between her and her lawyer," another plaintiff's "phone contained information from his work as a journalist," and

another plaintiff's "phone was a work phone officially owned by NASA's Jet Propulsion Laboratory," the ruling said. Federal officials did not dispute that they retained information that they got from these searches of electronic devices.

Multiple plaintiffs had their electronic devices seized during the border searches, although they were later returned.

The ruling noted that the harm to plaintiffs from the searches is ongoing, as "agents have the potential to access information on a traveler's past searches and… such information may be used to inform decisions on future searches."

The ruling includes this example:

> *The recent additional search of [plaintiff Suhaib] Allababidi's devices on July 6, 2019, furthers plaintiffs' argument as to the risk of future harm. Allababidi had previously been subject to a border search on January 24, 2017. When he declined to provide the password to his locked phone, CBP seized it to conduct an examination. On July 6, 2019, Allababidi arrived at the Toronto airport for a flight to Dallas, traveling with a smartphone and a laptop. CBP officers searched both devices. That such search of electronic devices continues for plaintiffs, even in the midst of their ongoing legal challenges to same, serves as further, undisputed indication of the sufficient likelihood that, unremedied, such alleged harm will continue in the future, particularly given the plaintiffs' future plans for international travel.*

The government told the court that electronic-device searches were conducted on .007% of the hundreds of millions of international travelers processed by CBP in 2017. But the judge wrote that "the number of reported electronic devices likely is underestimated" because of apparent shortcomings in how CBP calculates its data and because "ICE does not maintain

records of the number of basic searches that it conducts." The judge concluded that "the likelihood of plaintiffs having their electronic devices searched without cause is not a remote risk."

https://arstechnica.com/?p=1601063

Amazon gains unfair edge by making sellers use its shipping, complaint says



Enlarge / The Amazon logo at the entrance of a logistics center in France, July 2019.

reader comments

71 with 50 posters participating

Share this story

Amazon has come quite a way from when it was just an online bookstore, but it still operates a booming retail business among all its other ventures. A majority of the retail products sold on Amazon aren't actually sold *by* Amazon at all but rather by its sprawling network of third-party "marketplace" vendors. The company's relationships with those vendors, foreign and domestic, are at the center of a web of investigations and criticism.

Third-party retailers accounted for about 58% of Amazon's retail activity in 2018, company CEO Jeff Bezos said earlier this year, and they sold a cumulative $160 billion worth of goods. But those goods are sold in a "flea market" environment with minimal quality control, leading to ubiquitous counterfeits or recalled goods available for sale from fly-by-night merchants. If something goes wrong with your sale, getting recourse from these sellers is impossible.

Risky imports

All those kinda shady Amazon listings from companies in China you never heard of? They're not a bug, The Wall Street Journal reports today. They're a feature, present by design.

Amazon began a deliberate campaign in 2013 urging businesses in China to use its platform to sell directly to international customers, the WSJ writes. In 2017, an Amazon sales director based in China told business leaders in that country, "We help factories directly open accounts on Amazon and sell to US customers directly. This is our value."

The company made its website fully available in Mandarin in

2015, and by 2016, its team for recruiting and helping Chinese vendors was up to 150 employees, a former Amazon employee told the WSJ.

Earlier this year, the Journal found thousands of defective, recalled, or banned items for sale on Amazon. Those goods were sold by thousands of different merchants. Of the nearly 2,000 the WSJ could identify addresses for, 54% were based in China.

As of October, about 38% of the 10,000 most-reviewed merchant accounts on Amazon were based in China, analysts found; that number was around 25% in 2016. The WSJ and analytics firm Marketplace Pulse had to discern the business locations from their merchant pages on Amazon's Mexico site, as vendors are not required to disclose their locations on the US site.

Amazon disputed the WSJ's number, calling it "a significant exaggeration of the real percentage of the top 10 thousand." Amazon, however, did not provide a different number.

Meanwhile, new product listings appear on Amazon from China every 1/50th of a second, according to the WSJ, and that comes with some headaches. "Concerns at Amazon about Chinese listings arose several years ago in its China team, which noticed that, as local sellers flocked to the platform, it saw increasing patterns of fraud, counterfeits, and unsafe products," former Amazon employees based in China told the WSJ.

"Bad actors make up a tiny fraction of activity in our store and, like honest sellers, can come from every corner of the world," Amazon told the WSJ in response. "Regardless of where they are based, we work hard to stop bad actors before they can impact the shopping or selling experience in our store."

When Amazon's the bad actor

Amazon's handling of its US marketplace vendors, meanwhile, is

under deep scrutiny by federal regulators. Bloomberg recently obtained a letter one Amazon merchant sent to the House Antitrust Subcommittee, which is investigating Amazon, accusing the company of anticompetitive acts.

The letter "accuses Amazon of tying its marketplace and logistics services together," Bloomberg reports—using dominance in one business market to gain leverage in another, in a way that violates competition law.

Amazon has focused intensely on increasing its own in-house shipping business in recent years, and it now contracts with hundreds of third-party last-mile firms to get products from its warehouses to your door. That Prime-branded delivery service has continued to grow as competitors such as FedEx have stopped working with Amazon.

The merchant alleges that fees for using Amazon logistics have increased by 20% over the past four years and now cost as much as 35% more than competing services. But vendors are forced into paying the higher fees and using Amazon anyway, the complaint says, because Amazon promotes discovery for products it can mark as "fulfilled by Amazon" and demotes those that are not.

"The sticks Amazon uses to coerce merchants to use its logistics services are strict penalties, including getting kicked off the platform, for merchants who handle their own logistics," Bloomberg reports. "Merchants using Amazon logistics services aren't penalized when customer orders arrive late, even though they frequently do, since that's Amazon's responsibility. Those who handle their own logistics face stiff penalties for even minor delivery mishaps, including being suspended from selling on the platform," the vendor alleges.

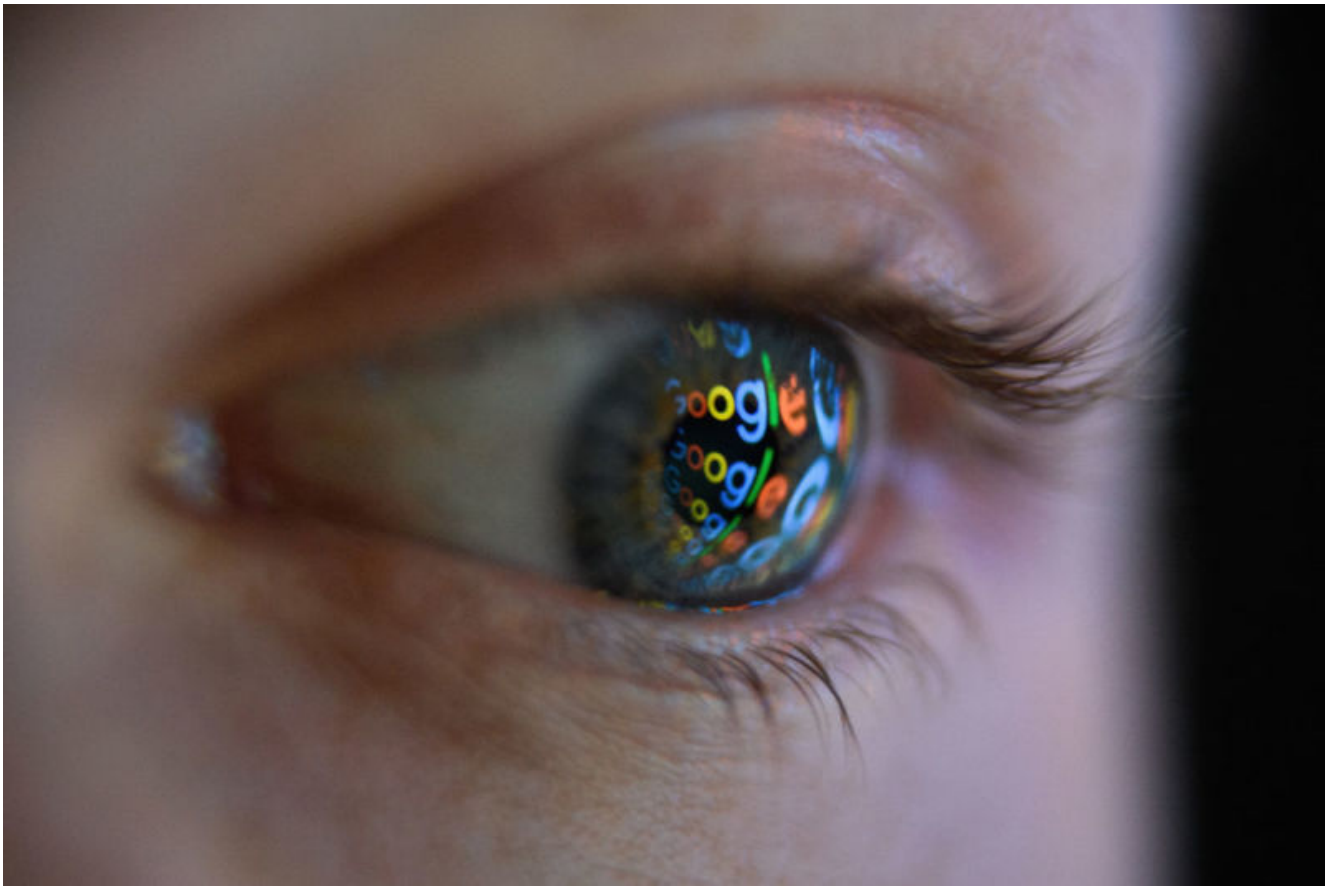
The claims come as Amazon faces antitrust probes in both the US and EU investigating its marketplace. Critics say that the

company collects data from third-party marketplace sales to choose what it should produce and promote in its own house brands.

“When providing a marketplace for independent sellers, Amazon continuously collects data about the activity on its platform,” the European Commission’s competition bureau said in July. “Based on the Commission’s preliminary fact-finding, Amazon appears to use competitively sensitive information—about marketplace sellers, their products and transactions on the marketplace,” to boost its own sales.

https://arstechnica.com/?p=1600799

Google: You can trust us with the medical data you didn’t know we already had



reader comments

137 with 87 posters participating

Share this story

Google now has access to detailed medical records on tens of millions of Americans, but the company promises it won’t mix that medical data with any of the other data Google collects on consumers who use its services.

Google provided this statement yesterday shortly after The Wall Street Journal reported that Google is partnering with Ascension, the country’s second-largest health care system, “on a project to collect and crunch the detailed personal-health information of millions of people across 21 states.”

“To be clear: under this arrangement, Ascension’s data cannot be used for any other purpose than for providing these services we’re offering under the agreement, and patient data

cannot and will not be combined with any Google consumer data," Google said in a blog post. That would mean Google won't use the medical data to target advertisements at users of Google services.

Google also said that its work with Ascension "adheres to industry-wide regulations (including HIPAA) regarding patient data, and come[s] with strict guidance on data privacy, security, and usage."

"We have a Business Associate Agreement (BAA) with Ascension, which governs access to Protected Health Information (PHI) for the purpose of helping providers support patient care," Google said. "This is standard practice in health care, as patient data is frequently managed in electronic systems that nurses and doctors widely use to deliver patient care."

What can Google see? Pretty much everything

Patient data shared with Google includes names, birth dates, addresses, family members, allergies, immunizations, radiology scans, hospitalization records, lab tests, medications, medical conditions, "and some billing claims and other clinical records," according to a followup article in the Journal. The partnership "covers the personal health records of around 50 million patients of Ascension," the Journal wrote.

The Journal said that "Neither doctors nor patients have been formally notified of the arrangement" and that Google and Ascension began the project "in secret last year."

Google seems to be correct that the partnership doesn't violate HIPAA (the Health Insurance Portability and Accountability Act). As the Journal noted, that law "generally allows hospitals to share data with business partners without

telling patients, as long as the information is used ‘only to help the covered entity carry out its health care functions.'” An expert quoted by the Journal noted that Google would be at risk of violating the law “if it uses the health data to perform independent research outside the direct scope of patient care.”

Ascension is not paying Google for these services, the Journal wrote, but Google’s work with Ascension could lead to profitable ventures. Google is using Ascension’s patient data “in part to design new software, underpinned by advanced artificial intelligence and machine learning, that zeroes in on individual patients to suggest changes to their care,” the Journal wrote. Google could sell this software to other health care institutions. As part of the project, “Staffers across Alphabet Inc., Google’s parent, have access to the patient information, internal documents show,” the Journal wrote.

The news about Google’s work with Ascension comes as Google is trying to buy Fitbit for $2.1 billion, in a deal that is pending regulatory approval. Fitbit devices are used for health tracking, among other things, and Google wants to use Fitbit to bolster its existing Wear OS platform.

But Google’s privacy promise should mean that it won’t combine any patient data from Ascension with the data it gathers from Fitbit, Wear OS, Google search, Gmail, Google Docs, Chrome, or any of the other consumer services it provides.

Update: The Google/Ascension project is now being investigated by the Office for Civil Rights in the Department of Health and Human Services, the Wall Street Journal reported in another story published at 7:02pm ET. The office said it “will seek to learn more information about this mass collection of individuals’ medical records to ensure that HIPAA protections were fully implemented.”

Google’s services for Ascension

Google said it is providing its standard G Suite productivity tools to Ascension and that it’s doing custom work for the company. This includes moving Ascension’s “on-premise data warehouse and analytics environments to their own private and secure Google Cloud environment.” The arrangement also includes “provid[ing] tools that Ascension could use to support improvements in clinical quality and patient safety,” Google said.

Google said its work with Ascension is similar to what it was already doing with “dozens of other health care providers.”

“These organizations, like Ascension, use Google to securely manage their patient data, under strict privacy and security standards. They are the stewards of the data, and we provide services on their behalf,” Google said.

Ascension also released a statement on its work with Google yesterday. Ascension said it aims to improve the tools used by both patients and caregivers as well as “explor[e] artificial intelligence/machine learning applications that will have the potential to support improvements in clinical quality and effectiveness.”

https://arstechnica.com/?p=1600915

Google has access to detailed health records on tens of

millions of Americans



Enlarge / Mountain View, Calif. – May 21, 2018: Exterior view of a Googleplex building, the corporate headquarters complex of Google and its parent company Alphabet Inc.

reader comments

155 with 95 posters participating

Share this story

Google quietly partnered last year with Ascension—the country's second-largest health system—and has since gained access to detailed medical records on tens of millions of Americans, according to a November 11 report by The Wall Street Journal.

The endeavor, code-named "Project Nightingale," has enabled at least 150 Google employees to see patient health information, which includes diagnoses, laboratory test results,

hospitalization records, and other data, according to internal documents and the newspaper's sources. In all, the data amounts to complete medical records, WSJ notes, and contains patient names and birth dates.

The move is the latest by Google to get a grip on the sprawling health industry. At the start of the month, Google announced a deal to buy Fitbit, prompting concerns over what it will do with all the sensitive health data amassed from the popular wearables. Today's news will likely spur more concern over health privacy issues.

Neither Google or Ascension has notified patients or doctors about the data sharing. Ascension—a Catholic, non-profit health system—includes 34,000 providers who see patients at more than 2,600 hospitals, doctor offices, and other facilities across 21 states and the District of Columbia.

The massive data-sharing project with Google has multiple objectives. For Google's part, the company is developing new software that employs artificial intelligence and machine learning to make care suggestions for individual patients. Google's ultimate goal is to develop a searchable, cloud-based tool to host and examine massive amounts of patient data—which it could then market to other health systems.

Ascension aims, in part, to improve patient care with the project. Internal documents seen by WSJ indicate that Ascension also hopes that the Google-mining will help identify additional ways to generate revenue from patients, such as ordering more medical tests.

Transforming care

In a statement, Ascension's Executive Vice President of Strategy and Innovations, Eduardo Conrado, said:

> *As the healthcare environment continues to rapidly evolve, we*

> *must transform to better meet the needs and expectations of those we serve as well as our own caregivers and healthcare providers. Doing that will require the programmatic integration of new care models delivered through the digital platforms, applications, and services that are part of the everyday experience of those we serve.*

Tariq Shaukat, president of Google Cloud, added in the statement that, by working in partnerships, Google hopes "to transform the delivery of healthcare through the power of the cloud, data analytics, machine learning, and modern productivity tools—ultimately improving outcomes, reducing costs, and saving lives."

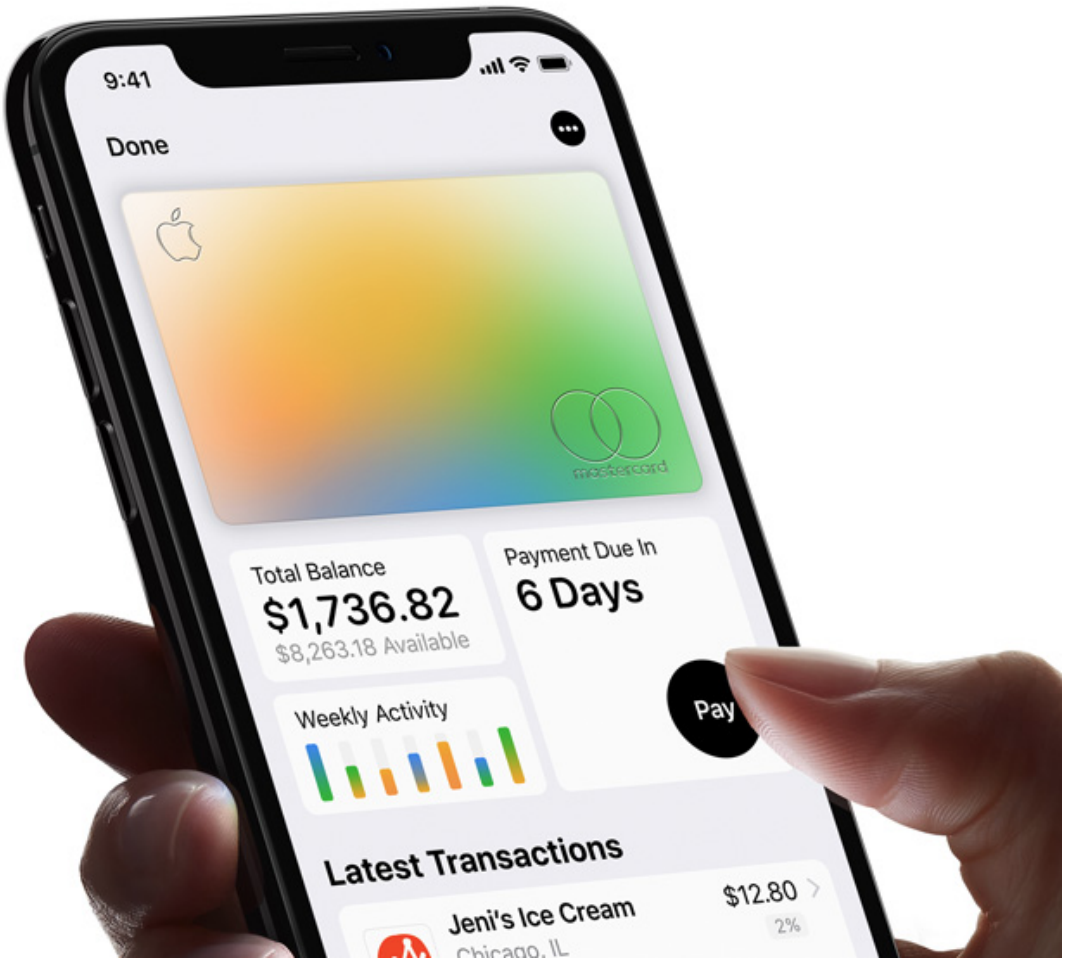
Both Google and Ascension said that the project is compliant with federal health information privacy protections and is "underpinned by a robust data security and protection effort."

Health privacy experts told WSJ that the project appears to be legal under the federal Health Insurance Portability and Accountability Act of 1996 (HIPPA). As the newspaper notes, the law "generally allows hospitals to share data with business partners without telling patients, as long as the information is used 'only to help the covered entity carry out its health care functions.'"

https://arstechnica.com/?p=1600565

NY regulators investigating Apple Card after viral

complaint of sexism



Enlarge / A dashboard built into iOS on iPhones lets you manage your card.

reader comments

122 with 78 posters participating

Share this story

Apple launched its own branded MasterCard nationwide in August. In the months since, the digital-first payment system has won some fans for its easy integration into the iPhone and Apple ecosystem, and it more or less seemed to work about as well as any other credit card. Now, however, financial-services regulators want to know what's going on under the hood amid accusations that the software determining the card's

terms has a sexist slant.

What happened?

Software developer and entrepreneur David Heinemeier Hansson took to Twitter late last week to complain about his wife Jamie Heinemeier Hansson's experience with AppleCard.

"The @AppleCard is such a fucking sexist program," his lengthy thread began. "My wife and I filed joint tax returns, live in a community-property state, and have been married for a long time. Yet Apple's black box algorithm thinks I deserve 20x the credit limit she does. No appeals work."

"It gets even worse," he added, sharing a screenshot showing $0 owed on a limit of, apparently, $57.24. "Even when she pays off her ridiculously low limit in full, the card won't approve any spending until the next billing period. Women apparently aren't good credit risks even when they pay off the fucking balance in advance and in full."

Speaking with Apple customer service did no good, he added, with representatives repeatedly deflecting blame to the black box that makes the determinations. Customer service representatives were, "very nice, courteous people representing an utterly broken and reprehensible system," Hansson said. "The first person was like 'I don't know why, but I swear we're not discriminating, IT'S JUST THE ALGORITHM.' I shit you not. 'IT'S JUST THE ALGORITHM!'"

Several other men on Twitter chimed in with replies outlining similar experiences. They said their wives, who on paper look like the better credit risks, received significantly less favorable terms on their Apple Cards than they did. One of the responses came from Apple co-founder Steve Wozniak, who tweeted that, although he and his wife have only joint bank accounts and assets, his Apple Card was given a limit 10 times higher than his wife's.

As Hansson’s thread went viral and gained media attention, representatives of Apple VIP customer service stepped in. They bumped the credit limit on Jamie’s card up to match David’s and launched an internal investigation.

External investigation

Apple VIP support aren’t the only ones interested in figuring out if the company’s mysterious algorithm is behaving in discriminatory ways; regulators are investigating now, too.

Hansson’s tweets drew the attention of Linda Lacewell, head of the New York Department of Financial Services. “Here in New York State, we support innovation,” Lacewell wrote in a blog post Sunday, adding:

> *However, new technologies cannot leave certain consumers behind or entrench discrimination. We believe innovation can help solve many challenges, including making quality financial services more accessible and affordable. Yet, this can’t be accomplished without maintaining public confidence. For innovation to deliver lasting and sustained value, the consumers who use new products or services must be able to trust they are being treated fairly.*

All financial products and services offered in New York State are required not to discriminate against protected groups. Those products include the Apple Card, which is backed by New York-based Goldman Sachs.

Goldman Sachs issued a statement Sunday saying the discrepancies happened because credit decisions are made on an individual basis, not taking family factors into account.

“We look at an individual’s income and an individual’s creditworthiness, which includes factors like personal credit scores, how much debt you have, and how that debt has been managed,” the company said. “Based on these factors, it is

possible for two family members to receive significantly different credit decisions. In all cases, we have not and will not make decisions based on factors like gender."

CNBC reports that Goldman was "aware of the potential issue" before the card launched in August but chose to move forward anyway. The bank says it is still considering ways of launching shared accounts, including adding multiple cardholders to a single account or allowing for co-signers.

The statement (and the potential for joint accounts or co-signers) does not specifically address why several users reported their wives—in some cases literal millionaires—were given significantly lower Apple Card credit limits and higher interest rates despite being the higher-income earners in the family, having higher credit scores, or both.

Unintended consequences

It's unlikely in the extreme that someone at either Apple or Goldman Sachs sat down, twirled his mustache à la Snidely Whiplash, and said, "Ah ha! Let's treat women more badly than men!" Doing so would be both morally and economically stupid, and nobody's accusing the companies of doing it intentionally.

Decisions made by algorithm, though, have a way of reflecting good old-fashioned human biases—just with even less transparency. And it happens in almost every field. The examples are becoming countless.

About a year ago, Amazon had to stop using an AI tool for hiring and recruiting purposes after it turned out not to be advancing female candidates. Essentially, the software looked at the company's current successful workforce, which skews male, and decided "male" must be a determinant of success.

In 2015, ProPublica discovered that Asian American families were likely to be charged significantly more for SAT test-prep

services. The algorithm determining price wasn't built expressly to discriminate by race; instead, it used ZIP code—but it charged higher rates in neighborhoods that turned out to be predominantly Asian.

Algorithms with systemic biases are also pervasive in the criminal justice system, where math tends to assign black criminals a higher chance of recidivism after serving their terms than white criminals, as well as higher cash bail, despite evidence showing the scores are unreliable and often wrong.

"The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants," ProPublica wrote in 2016. "White defendants were mislabeled as low risk more often than black defendants."

High-profile luck

The Hanssons are lucky in several ways. First, they're at about the highest end of the consumer spectrum. Jamie wrote in a statement today that she has been financially successful, independent of her husband, for a number of years. She does currently hold a full-time job outside of the home while caring for their three children, she said, but "I am still a millionaire who contributes greatly to my household and pays off credit in full each month." Both Hanssons have also repeatedly said in public that her credit score is not only excellent but also higher than his.

Beyond that, David has a high profile in the tech and business worlds, with lots of acquaintances and allies in all the right places and more than 350,000 Twitter followers. He can make a stink that will be both seen and taken seriously. The Apple Card is a luxury good, and the Hanssons got such a strong response, in short, because they have just about every privilege in the book—and they're both keenly aware of it.

“This situation… does not matter for my livelihood,” Jamie wrote in her statement, acknowledging, “This is not merely a story about sexism and credit algorithm blackboxes, but about how rich people nearly always get their way. Justice for another rich white woman is not justice at all.”

Instead of being about her specifically, she wrote, it’s the principle of the thing: “We cannot bow down to the algorithms. We cannot keep sliding into a *Black Mirror* world. Apple can and should be better than this. We should all be better than this.”

“I hear the frustration of women and minorities who have already been beating this drum loudly and publicly for years without this level of attention,” she added. “I didn’t wish to be the subject matter that sparked these fires, but I’m glad they’re blazing.”

https://arstechnica.com/?p=1600217