Comcast is trying to “dismantle” Civil Rights Act of 1866, MLK’s daughter says



Enlarge / Bernice King, daughter of Martin Luther King Jr. and CEO of the King Center, speaks during the Martin Luther King Jr. Annual Commemorative Service at Ebenezer Baptist Church on January 21, 2019 in Atlanta, Georgia.

reader comments

88 with 62 posters participating, including story author

Share this story

As a case involving Comcast and an African American-owned TV network operator heads to the US Supreme Court, a daughter of

Martin Luther King Jr. has accused Comcast of trying to "dismantle" the Civil Rights Act of 1866.

Bernice King, MLK's daughter and CEO of the King Center for Nonviolent Social Change, wrote an open letter to Comcast CEO Brian Roberts on Friday. She wrote that Comcast's argument at the Supreme Court would change the law to let businesses discriminate based on race.

"To alter the Act to accommodate discrimination against people based on race would reverse precarious progress in the freedom struggle, which my father was assassinated for leading and which my mother continued to join others in leading until her death," King wrote. She also told Roberts that "Comcast's ongoing pursuit to effectively dismantle a fundamental America[n] anti-discrimination law may be the legacy history forever associates [with] the company and your legacy of leadership."

> *Letter from King Center CEO, @BerniceKing, to @comcast Chairman/CEO Brian Roberts, with the Congressional Black Caucus CC'd. #RacialDiscrimination #EconomicInclusion #CivilRightsActOf1866 pic.twitter.com/oe9z7XaXbU*
>
> *— The King Center (@TheKingCenter) November 10, 2019*

King's letter pertains to a lawsuit filed against Comcast by Byron Allen's Entertainment Studios Networks (ESN), which claimed that Comcast's refusal to carry ESN channels was racially motivated and seeks a $20 billion judgment. Allen won a key decision in November 2018 at the US Court of Appeals for the 9th Circuit, which ruled that the case can move forward to a trial and that a US District Court had improperly granted Comcast's motion to dismiss ESN's complaint.

Comcast asked the Supreme Court to take up the case, and the court agreed to do so. A hearing is scheduled for Wednesday this week.

The key question is whether Allen must prove that racism was the primary factor motivating Comcast. Comcast told the Supreme Court that Allen's claim must "fail in the absence of but-for causation."

A "but-for" test asks, "but for the existence of X, would Y have occurred?" If the but-for standard is applied, Allen's suit would fail as long as a factor other than racism can explain Comcast's refusal to pay ESN to carry its TV channels, even if there is reason to think that Comcast was also motivated by racism.

"As this case goes before the Supreme Court, Comcast, under your leadership, seeks a ruling requiring plaintiffs prove discrimination was the only factor in the denial of a contract," King wrote to Roberts.

Given that, King told Roberts that Comcast should answer the following questions:

- *Knowing that the Civil Rights Act of 1866 was enacted to prohibit discrimination of any kind when making and enforcing contracts, why is Comcast relentlessly fighting for the right to avoid doing business with a person of color so long as her or his race is one of several factors for such refusal?*
- *Are you prepared to say business decisions based on racism are acceptable if combined with other non-racist reasons?*
- *Do you believe in your heart racism in modest doses should be permitted in American society, let alone in business contracts?*

King also said that Comcast's position in the case is at odds with its recent statement that "promoting diversity and inclusion are core objectives across our company."

Pressure from lawmaker

Comcast is also facing pressure from US Rep. Bobby Rush (D-Ill.), who told Roberts in a letter that Comcast "has shown itself to be an enemy of minority communities" and that the company should be broken up.

The National Association for the Advancement of Colored People took no position on the underlying dispute between ESN and Comcast but said that Comcast's legal argument would "roll back the crucial protections of one of the nation's oldest civil rights laws." Notably, the original version of ESN's lawsuit named the NAACP as a defendant along with Comcast. ESN alleged that the NAACP helped Comcast "whitewash" its discriminatory business practices by entering into a memorandum of understanding on diversity issues with the company, but the NAACP was later dropped from the case.

The US Department of Justice supported Comcast's position on but-for causation in a brief to the Supreme Court. The brief said that "But-for causation is the default rule for federal anti-discrimination laws."

Comcast defends legal argument and its record

When contacted by Ars today, Comcast called ESN's lawsuit "frivolous" and "baseless."

"All we are asking is that section 1981 in our case be interpreted the same way it has been interpreted for decades across the country," Comcast said. That's a reference to Section 1981 of the Civil Rights Act of 1866, which prohibits racial discrimination in contractual relationships.

Comcast said that the 9th Circuit decision was an "outlier," as courts have repeatedly upheld the but-for causation

standard in Section 1981 cases for decades. Comcast also said:

> *We have been forced to appeal this decision to defend against a meritless $20 billion claim, but have kept our argument narrowly focused. This case cannot detract from Comcast's strong civil rights and diversity record or our outstanding record of supporting and fostering diverse programming from African-American owned channels. There has been no finding of discriminatory conduct by Comcast against this plaintiff by any court, and there has been none.*

Comcast noted that it has reached programming deals with numerous African American-owned TV networks.

Opposing arguments

SCOTUSBlog published an in-depth summary of Comcast and Allen's arguments last week. As detailed on SCOTUSBlog by reporter Amy Howe, a lawyer who has argued Supreme Court cases, the Civil Rights Act of 1866 says that everyone must have the same rights as white people to make and enforce contracts. Howe summarized Comcast's argument as follows:

> *If the defendant would have made the same decision about whether to enter into a contract if the plaintiff had been white, Comcast reasons, then the plaintiff had the "same right" to enter into the contract. This interpretation is also consistent, Comcast suggests, with the Supreme Court's earlier cases interpreting the Civil Rights Act of 1866 as requiring the plaintiff to show that the decision in dispute was made "because of" the plaintiff's race—"language that unmistakably connotes but-for causation." Therefore, Comcast concludes, ESN's complaint must allege, and it must prove, that Comcast's decision not to enter into a contract would have been different were it not for the race of the company's owners.*

ESN argues that the Supreme Court in other cases endorsed a standard less stringent than “but-for causation” in Section 1981 claims.

“The justices have ruled that courts should use a ‘burden-shifting framework,’ which initially requires the plaintiff to provide evidence suggesting discrimination but then shifts the burden to the defendant to demonstrate that there is a legitimate and nondiscriminatory reason for its decision,” Howe wrote. “Congress, ESN argues, tacitly approved that standard when it amended parts of the Civil Rights Act in 1991 but ‘left the burden shifting holding of this decision untouched.'”

ESN also argued that “there was no tradition of requiring ‘but for’ causation in cases involving intentional torts, which are most analogous to Section 1981,” SCOTUSBlog wrote. “The cases that Comcast cites, ESN points out, involve allegations that the defendant was negligent, not that the defendant acted intentionally. Its interpretation, ESN continues, is also more consistent with Congress’ purpose in enacting the Civil Rights Act and Section 1981: to create a ‘sweeping’ bar on racial discrimination.”

Comcast and ESN both argue that a Supreme Court ruling in the other’s favor would have severe consequences. Comcast cautioned the court that if it doesn’t overturn the 9th Circuit ruling, “a party may be held liable for racially discriminatory contracting—and subjected to compensatory and punitive damages—even where it would have made the same contracting decision irrespective of race.”

“The defendant’s motives”

Meanwhile, ESN warned that a win for Comcast would prohibit a plaintiff “who alleges that race was a motivating factor for the refusal to contract” from conducting fact-finding on those claims if the plaintiff can’t meet the but-for causation

standard. That’s difficult, ESN said, because “the defendant typically is the only party with access to evidence of the defendant’s motives.”

“Comcast’s proposed pleading standard would effectively shut the door to the federal courts for African Americans and other people of color who are treated differently in contracting because of race,” ESN also told the Supreme Court.

ESN separately filed a similar lawsuit against Charter, the second-biggest cable company in the US after Comcast. Charter’s own petition to the Supreme Court is still pending, but the Supreme Court’s decision on Comcast could have an impact on the Charter case. “[T]he parties anticipate the Supreme Court will hold Charter’s petition in abeyance pending the disposition of the Comcast case,” according to a joint status report filed last month at the US District Court for the Central District of California.

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

https://arstechnica.com/?p=1600253

How Airbnb’s fight to overturn a New Jersey law imploded



Enlarge / A crescent moon rises in the pre-dawn sky over the skyline of lower Manhattan and One World Trade Center in New York City on October 25, 2019 as seen from Jersey City, New Jersey.
Gary Hershorn | Getty Images

reader comments

98 with 68 posters participating

Share this story

Residents of Jersey City, New Jersey, voted overwhelmingly in favor of strict short-term rental regulations on Tuesday, putting an end to the high-profile feud between Airbnb and local officials that had engulfed the city in recent months. The move comes as a major blow to Airbnb, which spent more than $4.2 million blanketing Jersey City in television ads, handouts, and pro-Airbnb canvassers in a campaign to quash the restrictions, which will affect a popular destination for guests looking to visit Manhattan (which is just across the Hudson River and several minutes away on public transit)

without running afoul of New York’s tight rules on short-term rentals.

The new rules crack down on Jersey City’s booming short-term rental industry—which has grown by an order of magnitude since city officials effectively legalized the practice in 2015—by requiring that owners obtain permits and limiting who can rent out their spaces and for how long. Despite an aggressive opposition campaign, voters approved the regulations in a landslide, with current estimates suggesting nearly 70% voted in favor of the measure.

WIRED

Jersey City’s rejection of Airbnb suggests that the tide may be changing for the so-called tech unicorn, as the city joins the growing ranks of former Airbnb defenders turned defectors. Local government officials around the nation that had been early advocates of the company, from Arizona and Louisiana to Oregon, are now turning against it. And with Airbnb looking to do an IPO in 2020—a process that involves airing out its dirty laundry for investors—every bit of regulatory backlash counts.

Airbnb has spent much of the last decade fighting for legitimacy in cities around the nation, earning the startup an infamous reputation among many local officials as a deep-pocketed agitator prone to litigation and public influence operations. The company has sued cities such as Boston, Miami Beach, Santa Monica, and even its hometown of San Francisco over ordinances beefing up short-term rental regulations, and it has spent hundreds of thousands of dollars hiring signature gatherers to help overturn local restrictions on both coasts.

However, over the years, the home-sharing giant began leaning more toward the carrot than to the stick. It has found success in many localities by partnering with local officials and agencies where each party ostensibly benefits. Airbnb began

striking deals with city and state officials to collect and remit some difficult-to-collect taxes from hosts in 2014, with new rules legalizing home-sharing in the area often announced by local officials either simultaneously or shortly after.

Jersey City was one of the first to announce such a deal. In 2015, Mayor Steve Fulop entered into an agreement with Airbnb that was estimated to potentially earn the city up to $1 million in occupancy tax revenue a year. In exchange, Airbnb worked to get Jersey City officials to implement rules legalizing short-term rentals. Airbnb touted its work with Jersey City as an exemplary partnership, highlighting it at length in PR materials concerning regulations in the following years. At the time of the agreement, Jersey City officials lauded Airbnb and explicitly encouraged the use of the platform generally in statements issued at the time.

City officials now say that the legalization of short-term rentals was a grave mistake. When the deal was struck in 2015, there were around 300 active Airbnb listings in Jersey City. Within one year, that number had grown to roughly 2,000, according to an Airbnb press release from December 2016. At present, there are upward of 3,000 Airbnb listings in Jersey City, the majority of which are whole-home rentals—where the owner isn't present during the guests' stay—and are operated by hosts that run multiple properties, according to data from Inside Airbnb, an independent site tracking the company. (Airbnb questioned the methods used to collect the data but did not provide WIRED with any evidence disputing the claims.)

Officials say that the boom converted precious housing stock into de facto hotels, resulting in higher rents, quality of life issues in neighborhoods plagued by transient occupants, and an exacerbated housing crisis. It's a concern echoed by many cities, as local government officials around the nation grapple with how best to handle the increasing popularity of short-term rental platforms like Airbnb, HomeAway, and VRBO in high-tourism areas.

In June 2019, the Jersey City council introduced a new ordinance aimed at remedying these issues. Starting in January 2020, rentals of a whole home or apartment where the owner isn't present are capped at 60 days a year; renters are largely barred from listing their homes on platforms like Airbnb and HomeAway; and short-term rentals are banned in many multifamily buildings, among many other provisions. The ordinance passed, but Airbnb poured money into the city to gather resident signatures in opposition. Within 20 days of the ordinance's passage, the company gathered more than 20,000 signatures, forcing a referendum.

"This administration is fighting to fix the quality of life issues our residents have had to endure over the years as Airbnb abuses their initial agreement with the city," Mayor Fulop said in a statement. "We're fighting to maintain affordable housing for those who need it most. We're fighting to rid residential buildings of party hotels."

In the lead-up to the vote Tuesday, Airbnb created a political action committee called Keep Our Homes, through which it spent some $4.2 million trying to convince the city's 265,000-some residents to oppose the measure. Though it failed in this instance, Airbnb has used these tactics successfully before in cities like San Diego—which had to withdraw short-term rental regulations in 2018, following a similarly high-profile signature gathering campaign led by Airbnb and other short-term rental platforms.

"Cities from Buffalo to San Francisco and Boston to Seattle have managed to pass comprehensive short-term rental regulations without punishing tenants or creating red tape and onerous registration systems," said Airbnb spokesperson Christopher Nulty, without mentioning Airbnb's initial opposition to San Francisco's and Boston's regulations, which ended only after the company settled the lawsuits it filed against each city. "It's unfortunate to see the hotel-backed special interests run a campaign that moves Jersey City in a

different direction.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1599381

GirlsDoPorn owner charged with child porn for scene with 16-year-old



reader comments

64 with 43 posters participating

Share this story

Michael Pratt, the principal owner of the GirlsDoPorn website, is already facing criminal charges for sex trafficking involving adult women. A new indictment, unsealed Thursday, has added child pornography charges.

For years, Pratt has been recruiting young women to San Diego to shoot pornographic videos. Dozens of women say that Pratt and his colleagues lied to them and used physical coercion to induce them to participate—claims that led to federal sex trafficking charges last month.

Now prosecutors say that Pratt flew a 16-year-old girl to Southern California to have sex on camera. That would be a violation of federal laws against production of child pornography as well as sex trafficking of minors.

It's not clear if Pratt will ultimately stand trial for his alleged crimes. Pratt, a New Zealand native, reportedly left the United States in September in the midst of a long-running civil trial that is still ongoing.

Criminal charges were filed against Pratt and three others in October. Two of Pratt's co-defendants are now in federal custody, while a third is out on bail. But Pratt is believed to be in New Zealand.

Courthouse News reports that the new indictment was unsealed at "a hearing attended by Pratt's co-defendants, GirlsDoPorn videographer Matthew Wolfe, actor Andre Garcia, and administrative assistant Valorie Moser." The judge entered a not guilty plea for the trio.

https://arstechnica.com/?p=1599605

Six arrested for selling Chinese gear to military as “Made in America”



Jan-Stefan Knick / EyeEm / Getty

reader comments

59 with 46 posters participating, including story author

Share this story

In August 2018, an Air Force service member noticed something strange about a body camera being used by security personnel at an Air Force base: Chinese characters on the screen. A subsequent investigation found numerous indications that the camera—and two dozen others in the same shipment—had been made in China.

Investigators found three telling logos in the camera's firmware: an Air Force Logo, the logo of the Chinese company that made the camera, and the logo of China's ministry of public security. Forensic analysis indicated that all three images had been loaded on the camera at the same time by someone in a Chinese time zone. This suggested that not only was the camera made in China, but the Chinese knew that the body camera would be shipped to an Air Force facility.

How did a Chinese-made digital camera wind up at a US Air Force base? In a criminal complaint unsealed Thursday, federal prosecutors blamed Aventura, a New York-based company that has been fraudulently re-selling Chinese-made gear for more than a decade. On Thursday, six of the company's founders and senior officials were arrested and charged with fraud and other crimes.

Passing off Chinese goods as "Made in America"

A federal law called the Trade Agreements Act restricts federal agencies from purchasing goods made in certain countries—including China. Federal law also requires companies to accurately disclose where products have been manufactured—especially when they're sold to federal agencies.

But since 2006, the feds say, Aventura has been buying Chinese-made cameras, metal detectors, and other products, slapping "Made in America" logos on them, and re-selling them in the United States—to customers including US government agencies who are legally prohibited from buying such items.

The complaint argues that the Aventura's senior executives—particularly managing director and *de facto* owner Jack Cabasso, knew exactly what they were doing. In 2016, in a remarkable display of chutzpah, Cabasso sent an email to a government official arguing that 12 of his competitors were

violating federal law by selling Chinese-made products to the federal government.

This, he wrote, was a “big problem” because the Chinese manufacturer was “actually the Communist Chinese government and had significant cybersecurity issues aside from TAA compliance.” Thursday’s complaint charges that Aventura had been re-selling gear made by the same Chinese company.

When a Qatari distributor emailed Aventura in 2018 to get confirmation that the company’s gear was US-made, Cabasso replied with a purported photo of Aventura’s manufacturing facility on Long Island, New York. He wrote that representatives of the Qatari distributor could visit the factory at any time.

In reality, the photo showed an image taken from a 2014 article published in a trade publication showing the Chinese facility where the camera had actually been manufactured.

Aventura allegedly went to significant effort to conceal the Chinese origins of its products. Email records show the company worked with its Chinese suppliers to scrub any reference to the original manufacturer from circuit boards and onboard software.

Still, Aventura’s efforts to conceal its gear’s origins was far from foolproof. One sample product was shipped to a prospective customer with a Chinese user manual included. In another case, a customer figured out that the camera was a modified version of a Chinese product and “asked Jack Cabasso to supply the original, unaltered firmware” created by the Chinese company “in the hopes that it would be superior to Aventura’s ‘buggy’ altered version.”

Company founders allegedly enjoyed

a lavish lifestyle

The feds say Aventura has earned $88 million in revenue over the last decade, including $20 million in federal contracts. “Aventura’s largest customers are US government agencies, including the US Army, US Navy, and US Air Force,” prosecutors report.

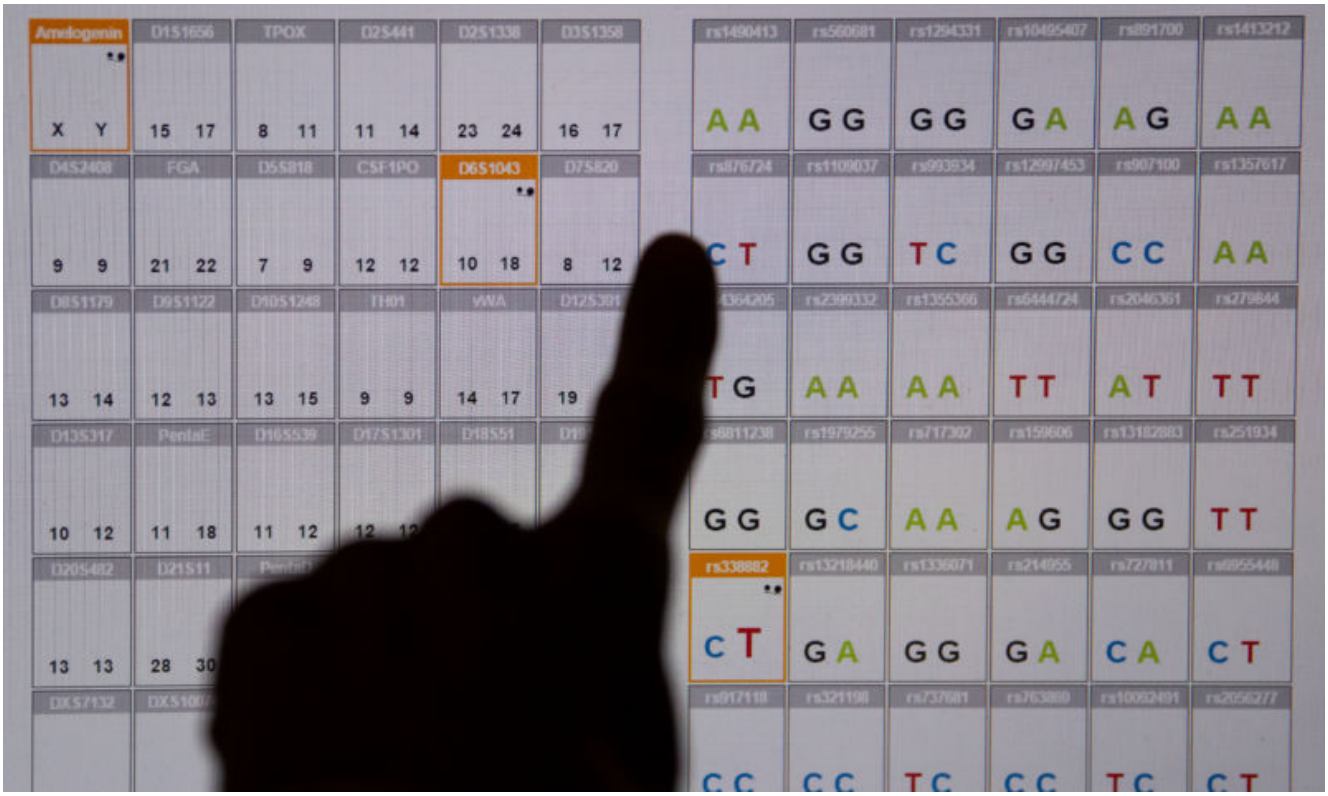
The Air Force body cameras weren’t the only case where sensitive Chinese-made gear ended up in military facilities. In another case, the Navy ordered a $13,500 night vision camera from Aventura. Federal investigators intercepted the camera as it arrived at JFK airport from China and discreetly marked it. The same camera was delivered at a naval base in Connecticut two weeks later.

The government charges that Aventura’s fraud allowed Jack Cabasso and his wife to live a lavish lifestyle. In 2016, the company wired $450,000 to help buy a house for one of the couple’s children. The couple has allegedly spent around a million dollars to maintain a 70-foot yacht.

The company even allegedly committed fraud to qualify as a woman-owned business. Federal law gives special contracting opportunities to companies that are owned and controlled by women. Jack’s wife Frances was listed as the majority shareholder and CEO of Aventura, but prosecutors say that she played virtually no operational role at the company. Instead, she had a full-time job at an unrelated accounting firm, according to federal prosecutors.

https://arstechnica.com/?p=1599191

Search warrant overrides 1M users' choice not to share DNA with cops



Enlarge / A DNA sequence analysis (genetic fingerprint) seen on a monitor in the Bavarian State Criminal Police Office in Munich, Germany.

reader comments

133 with 78 posters participating

Share this story

Law enforcement agencies around the country have for the past few years eagerly latched onto consumer-facing DNA sites as a rich repository of information to help them close cases. Many of those sites have been allowing users to adopt privacy settings and restricting what data they allow police to access, but a first-of-its-kind search warrant may blow those users' data banks wide open.

Police in Orlando, Florida, obtained a warrant this summer to search DNA site GEDmatch and review data on all of its users—about a million people, The New York Times reports. Privacy advocates are now concerned that police will continue to get broad warrants for DNA sites, including larger peers such as 23andme or Ancestry that have much larger pools of user data.

GEDmatch? Sounds familiar…

GEDmatch hit the spotlight in 2018, when DNA data from its site led to the eventual arrest of a man suspected to be the "Golden State Killer," responsible for dozens of rapes and murders in California between 1976 and 1986.

"Although we were not approached by law enforcement or anyone else about this case or about the DNA, it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy," site co-founder Curtis Rogers told Ars at the time. "It is important that GEDmatch participants understand the possible uses of their DNA, including information of relatives that have committed crimes or were victims of crimes," he added, saying that anyone not comfortable with that should delete their data from the site.

In the wake of that attention-grabbing case, GEDmatch changed its policies in May 2018 to make it less easy for police to access their data. Users now have to opt in to having their data made available to police; information they upload is set to private by default. Rogers told the NYT that as of October, less than 15% of current users, 185,000 out of 1.3 million, have opted in to sharing their data with police.

That limitation has frustrated law enforcement, though, and the Orlando detective in July asked a Florida judge to approve a warrant that would let him search the entire GEDmatch database regardless of users' privacy settings, and the judge

agreed. The site reportedly complied to the search demand within 24 hours.

Who generates the data?

GEDmatch, unlike its larger rivals, doesn't collect any DNA data itself. Instead, it relies on user uploads. In its terms of service, the company says acceptable data includes:

- *Your DNA*
- *DNA of a person for whom you are a legal guardian*
- *DNA of a person who has granted you specific authorization to upload their DNA to GEDmatch*
- *DNA of a person known by you to be deceased*
- *DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault*
- *DNA obtained and authorized by law enforcement to identify remains of a deceased individual*
- *An artificial DNA kit (if and only if: (1) it is intended for research purposes; and (2) it is not used to identify anyone in the GEDmatch database)*
- *DNA obtained from an artifact (if and only if: (1) you have a reasonable belief that the Raw Data is DNA from a previous owner or user of the artifact rather than from a living individual; and (2) that previous owner or user of the artifact is known to you to be deceased)*

That openness is why investigators prefer to use GEDmatch, the Times explains. That differentiates it from the larger services, 23andme and Ancestry, which perform DNA analysis themselves on samples that users send in.

23andme this week in a corporate blog post reiterated its

commitment to user privacy.

“If we had received a warrant, we would use every legal remedy possible” to challenge it and try to avoid turning over user data, the company’s chief legal and regulatory officer, Kathy Hibbs, wrote. “In our 13 year history, 23andMe has never turned over any customer data to law enforcement or any other government agency.”

According to its transparency report, since 2015, 23andme has received seven requests pertaining to 10 individuals and has shared data in response to none of them.

The weakest links

With DNA, arguably more than any other kind of data, your privacy is only as assured as your least privacy-minded relative wants it to be—and you might not even know that person. Thousands of users have discovered surprise half-siblings, unknown biological parents, or forgotten branches of their family trees out there in the world since services like 23andme became broadly popular.

Researchers in late 2018 found that about 60% of DNA samples from a consumer genealogy company could be linked to distant relatives. That number went up for users of white European descent, who were 30% more likely to be matched because the user base of the testing platform skews toward higher-income white consumers.

GEDmatch, meanwhile, seems to be an even riskier repository for all that sensitive data than some of its competitors. It has no hesitancy complying with search requests. “We may disclose your raw data, personal information, and/or Genealogy Data if it is necessary to comply with a legal obligation such as a subpoena or warrant,” the site’s privacy policy says. “We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless

notification is prohibited under law.”

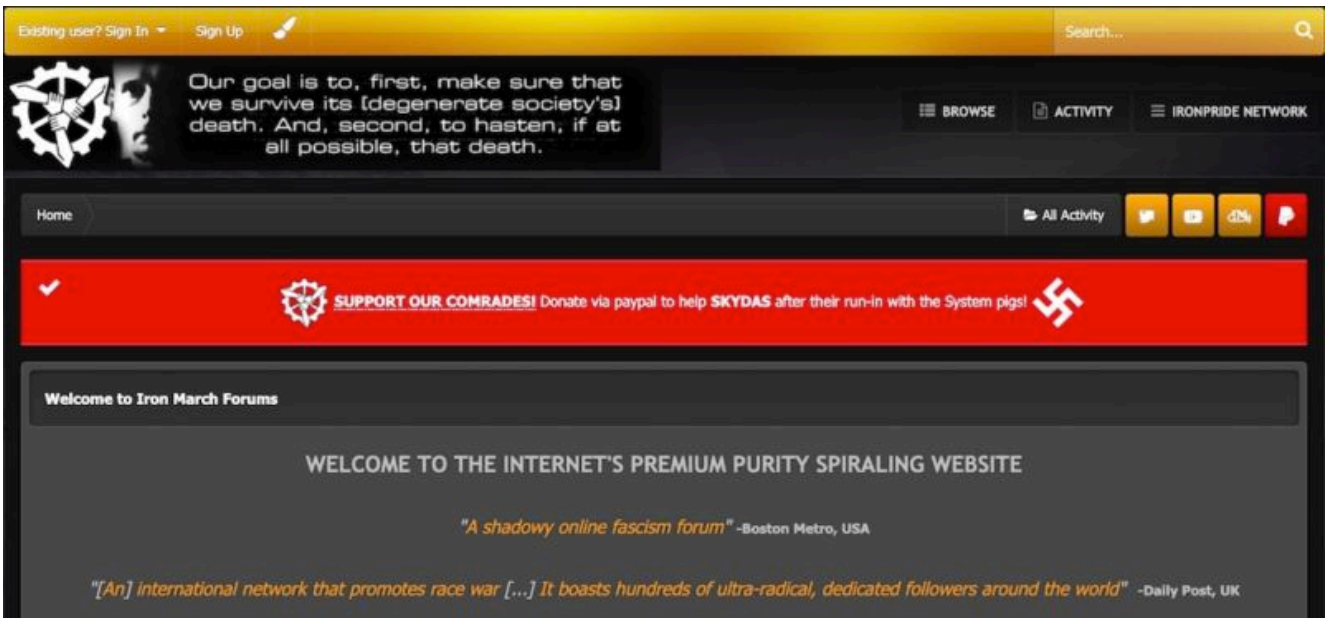
GEDmatch also has flaws in it that could allow a whole lot of unintentional access to genetic data, the MIT Technology Review recently reported. The site has apparently been subject to data scraping attempts which might constitute a national security threat, the report explains.

Rogers downplayed the risks, answering, “I don’t want to get into it,” when pressed about the data scraping.

“We certainly are concerned about privacy also, and it’s good that studies like this are done,” Rogers added in a statement to the Technology Review. “But no matter what you do, there will always be some potential for privacy invasion when you are doing genealogy. Genealogy is a procedure in which you want to compare your information to other people’s.”

https://arstechnica.com/?p=1598589

Members of violent white supremacist website exposed in massive data dump



reader comments

65 with 48 posters participating

Share this story

Editor's note: this article discusses a hate group's uses of racist language that may be hard to read.

Private data for Iron March, a notorious website for violent white supremacists, has been published online in a stunning leak that exposes a trove of detailed information on as many as 1,000 or more members. The 1GB SQL database appears to contain the entirety of the site's information, including user names, private messages, public posts, registered email addresses, and IP addresses.

The leak was posted on the Internet Archive on Wednesday by an anonymous individual using the handle antifa-data. A list of domains used in email registrations shows two from US universities. Private messages show some members discussing life in the US Marines, Navy, Army, and military reserves.

"Be careful if you get deployed with those fucking sand [deleted] and jews," a user claiming to be in the Navy tells another member who says he's in the Marines and is about to be

deployed. (The racist term he used has been deleted.) “They are all a bunch of slippery pieces of shit that wash their faces in rain puddles in dirt on the ground. We are too good to be interacting with those people, maybe trump will at least relax the ROE’s [rules of engagement] so those pieces of shit can be blasted back to allah, jews and all.”

To the right of the Alt-Right

According to the Southern Poverty Law Center and Rational Wiki, Iron March was launched in 2011 by Alexander “Slavros” Mukhitdinov, who is believed to be a Uzbekistani who emigrated to Russia. The fascist vision he espoused was critical even of the Alt-Right movement that gained visibility after the election of Donald Trump, the SPLC said, citing a review of more than 150,000 public Iron March posts it scraped from September 2011 to September 2017. The website went dark in 2017 for reasons that remain unknown.

Iron March was affiliated with or offered support to at least nine fascist groups in nine different countries over its six-year span. Several violent neo-Nazi paramilitary fascist groups were organized on the forums, including, the Antipodean Resistance and the Atomwaffen Division. Members and associates of the groups and their offshoots have been connected to at least five murders documented by the SPLC and Rational Wiki.

Among the fatal attacks, both sources say, was the brutal 2017 murder of activist Heather Heyer in Charlottesville, Virginia, on August 12, 2017. During the incident, James Alex Fields rammed his car into her after she had protested a “Unite the Right” rally. Fields, the SPLC said, had marched at the rally as a member of a group called Vanguard America, which descended from another Iron March group.

While the SPLC had already obtained all or at least most of Iron March’s public posts, the trove posted Wednesday is sure to offer a much more complete, and likely incriminating,

picture of one of the Internet’s most sordid forums. The ability for researchers, law enforcement investigators, and others to cross-reference IP addresses, email addresses, and private and public posts is likely to shine a bright light into a nether region that thrives on darkness.

The open source journalism collective Bellingcat has already established a forum for people to collaborate on research.

https://arstechnica.com/?p=1598725

Netflix CEO defends censoring anti-government video in Saudi Arabia



Enlarge / Comedian Hasan Minhaj in 2019.

reader comments

52 with 42 posters participating

Share this story

As 2019 began, Netflix suppressed an episode of comedian Hasan Minhaj's show *Patriot Act* for the Saudi Arabian market, sparking outcry from some Western critics. In a Wednesday interview, CEO Reed Hastings shrugged off those concerns.

"We're not in the news business," he said during an event sponsored by The New York Times. "We're not trying to do 'truth to power.' We're trying to entertain."

"We can accomplish a lot more by being entertainment and influence the conversation about the way people live, rather than being another news channel," he added.

Netflix removed the video at the request of the Saudi government, which said it violated a Saudi law prohibiting distribution of content that impinges on public order, religious values, or public morals.

The removal prevented some Saudis from watching the video, at least on Netflix's platform. But it remained available outside of Saudi Arabia. And Saudi censorship boosted Minhaj's profile in the United States.

"For the first time in my life, I was a bipartisan icon," Minhaj joked. "Liberals and conservatives: they both embraced me like I was money from Big Pharma."

Global media companies like Netflix face a difficult task balancing the competing demands of governments around the world. Free-speech purists would like companies to do more to fight censorship in repressive countries like Saudi Arabia. But there's a risk that a vigorous defense of free speech

could get a company like Netflix banned from countries like Saudi Arabia altogether, which could be an even worse outcome for freedom of speech.

https://arstechnica.com/?p=1598583

Massive Facebook document leak gives ammunition to investigators



Enlarge / Facebook CEO Mark Zuckerberg speaking about Facebook News in New York, Oct. 25, 2019.

reader comments

62 with 47 posters participating

Share this story

Facebook is facing a new round of intense scrutiny worldwide after 7,000 pages of confidential files stemming from a lawsuit were made public yesterday. Those documents are not the ones California's attorney general needs, though, so separately, the company is *also* facing a court challenge demanding it produce more documentation for an investigation amid allegations of stonewalling.

The piles of leaked documents, which directly reference the company's questionable position on competition, are likely to be extremely helpful to the dozens of entities currently investigating Facebook on antitrust grounds. California, however, is conducting a privacy investigation.

State Attorney General Xavier Becerra yesterday took to court seeking to have a subpoena against Facebook enforced. The petition (PDF) alleges Facebook failed to respond to repeated subpoenas and other legal requests for information related to the Cambridge Analytica scandal.

Attorneys general for 47 states have now signed onto a joint probe of Facebook—but California has been one of the very few not participating in that probe. Neither is it involved in a joint investigation of Google that 48 attorneys general have undertaken.

Becerra in a press conference told reporters, "Today, we make this information public because we have no choice." But he declined to provide details on any other aspect of this or any other possible Facebook investigation. He and all the other regulators and attorneys general, however, may find something worth reading in Wednesday's leak.

The data dump

The 7,000 pages of leaked information spring from a 2015 lawsuit filed against Facebook by a company called Six4Three.

Six4Three, long since defunct, basically operated an unmemorable app that scraped Facebook looking for pictures of women in bikinis. Facebook in 2014 changed the way a key API worked, effectively breaking Six4Three's app. The developer sued, alleging breach of contract and "fraudulent and anti-competitive schemes." And then things got weird.

UK regulators were also conducting a probe into Facebook at the time. A Six4Three executive was brought into a meeting with a member of Parliament in November 2018, where he reportedly "panicked" and suddenly handed over confidential files from the case, despite a warning from a California judge not to.

The suit itself got even more strange from there, but the cache of documentation took on something of a life of its own.

The documents have leaked in smaller chunks through the past year, revealing that Facebook not only engaged in extensive lobbying against privacy protection laws in the EU but also considered selling access to user data.

The full trove of files was eventually leaked to UK journalist Duncan Campbell, who shared the files with NBC News and a handful of other outlets earlier this year. Campbell and those news outlets eventually released the whole lot to the public yesterday.

The juicy new bits

The documents seem to confirm two long-held, popular suspicious about Facebook. First, it treats user privacy as an afterthought at best. And second, it works hard to prevent

competitors from getting too powerful.

“Switcharoo”

Facebook in 2014 made significant changes to the way developers were able to access user information through its APIs. The company needed a way to sell such a large-scale change, though, so it came up with a narrative: privacy.

Internal communications reveal that Facebook ultimately tied the change to a revision of another product: Facebook Login. In a March 2013 email, one executive, Justin Osofsky, wrote that the narrative “will focus on quality and the user experience which will potentially provide a good umbrella to fold in some of the API deprecations.”

The connection between the two was almost entirely for messaging, further emails show. In a November 2013 email, Ilya Sukhar, head of developer products until 2016, asked, “What does it actually mean to tie [the change] to login besides synchronized timing? Is it just the messaging? What’s the bullshit that you refer to?”

“Mainly messaging,” another executive replied.

Sukhar later described the plan as a “switcharoo,” writing in a Febuary 2014 email:

> *Hi guys, I invited you all to a doc that outlines the details of the “switcharoo” plan some of us have been knocking around. I think it is a good compromise given all the restraints, and we’ll be able to tell a story that makes sense.*

Killing competition before it hatches

Emails among Facebook executives in 2013 show that the company planned to split up apps and services it didn’t own into one

of three categories: current competition, potential future competition, or “developers that we have alignments with on business models.”

A series of email exchanges from 2013 also discuss in detail the choices Facebook made to prohibit potential competitors from advertising on its apps. The question of who qualified as competition—other than Google, which was taken as a given—was debated at length in the email thread.

Ultimately, company leadership seemed to settle on messenger apps being more of a threat than other types of services.

“I think we should block WeChat, Kakao, and Line ads,” company CEO Mark Zuckerberg wrote in a 2013 email. “Those companies are trying to build social networks and replace us. The revenue is immaterial to us compared to any risk. I agree we should use ads to promote our own products, but I’d still block companies that compete with our core from gaining any advantage from us.”

Another series of 2013 emails show how Facebook leadership handled new competition.

MessageMe, a messaging startup, launched in 2013 and was acquired by Yahoo in 2014. Right out of the gate, Facebook leadership considered MessageMe to be too much of a competitive threat to allow the company to access its data. But Facebook was keenly aware of how restricting MessageMe’s access would look from the outside.

“In the first week after launch, MessageMe actually didn’t make any friends.get calls,” Osofsky wrote. “However, MessageMe is now up to ~350K [monthly active users] and made 333K friends calls last week. We will restrict their access to friends.get shortly.”

Osofsky added that the company would also “see if there are any other messenger apps which have hit the growth team’s

radar recently. If so, we'd like to restrict them at the same time to group this into one press cycle."

Companies in that third bucket, however, were able to make deals with Facebook to re-secure access to user data after the API shift. Amazon, for example, was allowed in because it spent money on advertising with Facebook.

Investigator ammunition

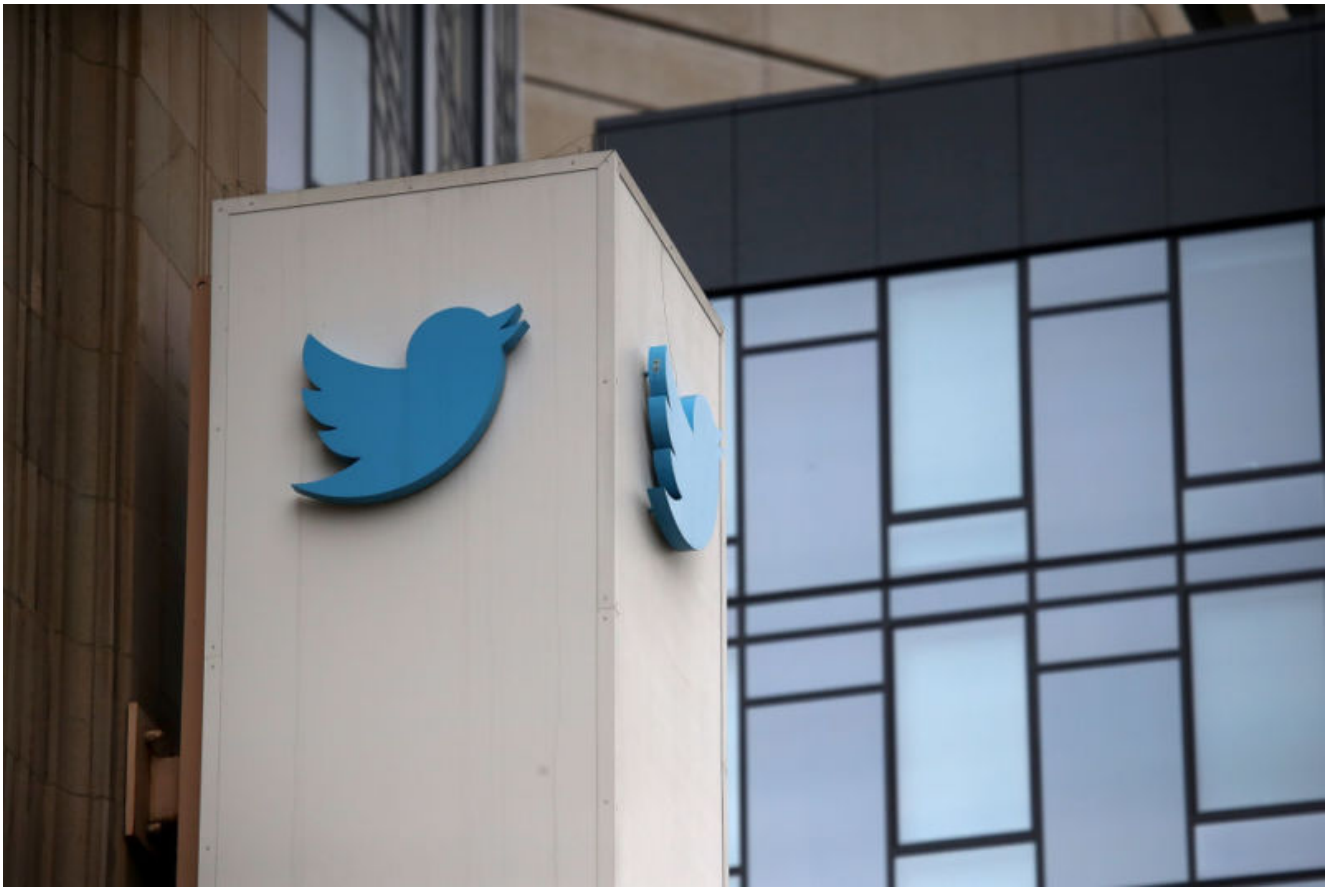
Facebook is currently the target of at least a half-dozen different antitrust probes. In the United States, the House Antitrust Subcommittee, the Federal Trade Commission, the Department of Justice, and 47 states attorneys general are all conducting investigations. European regulators are also working on their own competition cases against the behemoth.

Those probes are not solely addressing the question of whether Facebook is a monopoly, which is what most people associate with antitrust. Rather, they are focusing on *what Facebook has done* with the market power it has. In particular, using data a company such as Facebook collects from one arm of the business to prevent competitors from arising to challenge other arms of the business is the sort of behavior that antitrust regulators are getting out their metaphorical magnifying glasses to investigate in depth.

https://arstechnica.com/?p=1597577

Former Twitter employees

charged with spying on users for Saudis



Enlarge / While at Twitter, two men allegedly gathered data on users “of interest” to the Saudi Government and Crown Prince Mohammed bin Salman, the Department of Justice said in an indictment unsealed today.

reader comments

3 with 3 posters participating

Share this story

In an indictment filed on November 5, the Justice Department has charged two former employees of Twitter as acting as unregistered agents for the Kingdom of Saudi Arabia and falsifying documents provided to the Federal Bureau of Investigations to cover up their activities as spies working within Twitter. This is the first time the United States has

formally charged Saudis of spying in the US.

One of the former employees—Ahmad Abouammo, a US citizen who left Twitter in May 2015—was arrested on Tuesday. The second, a Saudi citizen named Ali Alzabarah, fled the country a day after being confronted about his activities and being placed on leave by Twitter in December 2015. A third individual—Ahmed al Mutairi, another Saudi citizen and the head of a Saudi social media company—acted as an intermediary for Bader Al Asaker, a man who is often referred to Crown Prince Mohammed bin Salman's "invisible hand."

Starting in 2014, Abouammo and Alzabarah worked with a Saudi government official identified by The Washington Post's Ellen Nakashima as Al Asaker. They passed internal Twitter data on users "of interest to [Al Asaker] and the Saudi Royal Family."

The data included email addresses and IP addresses associated with the accounts as well as devices and browsers used—providing tracking of the account users' movements. In some cases, the accounts included images that could have been construed as security threats—including images of improvised explosive devices—and Twitter removed the posts after emergency takedown requests from the Saudi government. In others, the accounts were merely critical of Mohammed bin Salman or the government.

After being placed on leave by Twitter, Alzabarah sent a letter of resignation while aboard a flight back to Saudi Arabia. Once he arrived there, he took a job with a charity led by Al Asaker called MiSK—a charity created by Mohammed bin Salman.

According to the affidavit from the FBI, Abouammo was paid at least $300,000 by Al Asaker for his work—payments he tried to cover up with faked invoices to his personal company, according to the FBI. The indictment alleges that Abouammo also received gifts, including a watch worth approximately

$20,000.

https://arstechnica.com/?p=1597869

New bill would create Digital Privacy Agency to enforce privacy rights



Enlarge / Chairwoman Anna Eshoo, D-Calif., conducts a House Energy and Commerce Subcommittee on Health markup on Thursday, July 11, 2019.

reader comments

22 with 21 posters participating

Share this story

Congress is taking yet another stab at addressing the near-complete lack of federal laws covering the absolutely massive trove of data that companies now collect on every one of us, which forms the backbone of basically the entire big tech era.

Representatives Anna Eshoo and Zoe Lofgren, both Democrats from California, introduced the Online Privacy Act today. The act would create a new federal agency, the Digital Privacy Agency, to enforce privacy rights. The act would also authorize the agency to hire up to 1,600 employees.

“Every American is vulnerable to privacy violations with few tools to defend themselves. Too often, our private information online is stolen, abused, used for profit, or grossly mishandled,” Eshoo said in a statement. “Our legislation ensures that every American has control over their own data, companies are held accountable, and the government provides tough but fair oversight.”

“Our country urgently needs a legal framework to protect consumers from the ever-growing data-collection and data-sharing industries that make billions annually off Americans’ personal information,” Rep. Lofgren added. “Privacy for online consumers has been nonexistent—and we need to give users control of their personal data by making legitimate changes to business practices.”

The Online Privacy Act

The provisions in the bill (PDF) would apply to “any entity (including nonprofits and common carriers) that intentionally collects, processes, or maintains personal information AND transmits personal information over an electronic network.”

Under the terms of the OPA, individuals would have the right to obtain, correct, and delete data collected about them by

covered entities, as well as to request “a human review” of automated decisions. Users would also have to opt-in to having their personal data used for training machine learning algorithms. They would be able to choose for how long companies retain their data.

The bill distinguishes between aggregated data and personal, identifiable data that is tied to an individual, and it places strong limitations on use of the latter. As outlined in a one-page fact sheet, the OPA would:

- *articulate the need for and minimize the user data [covered entities] collect, process, disclose, and maintain*
- *minimize employee and contractor access to user data*
- *not disclose or sell personal information without explicit consent*
- *not use third-party data to reidentify individuals*
- *not use private communications, (e.g., emails and Web traffic) for ads or other invasive purposes*
- *not process data in a way that violates civil rights, e.g., employment discrimination*
- *only process genetic information in limited circumstances*
- *use objectively understandable privacy policies and consent processes, and may not use ‘dark patterns’ to obtain consent*
- *employ reasonable cybersecurity policies to protect user data, and*
- *notify the agency and users of breaches and data-sharing abuses, e.g., Cambridge Analytica*

The privacy mess

Privacy law in the United States today is a patchwork of regulation, and the end result is basically a hot mess that

leaves agencies with limited authority to investigate and penalize even egregious abuses of personal data.

The federal statutes that exist each cover a specific, limited kind of data and enumerate a specific, limited kind of entity that's obligated to protect that data. So for example, while your doctor's office can't sell information about your diagnoses to a third party, no such limitation applies to apps or wearable devices that collect the same kinds of data.

A handful of states have additional laws on the books. Illinois, for example, adopted a prescient law back in 2008 that regulates the collection and use of individuals' biometric data. Facebook since 2015 has been embroiled in a class-action lawsuit in that state over its use of facial recognition.

The biggest player at the state level is California, which in 2018 adopted a sweeping privacy law that would give individuals more control over how their personal data is collected, used, and sold. That law has survived several attempts by opponents to weaken its key provisions, and it goes into effect on January 1.

Representatives Eshoo and Lofgren are far from the first to propose new federal legislation to address the morass. In fact, they're not even the first this year. Sen. Ron Wyden (D-Ore.) last month introduced the Mind Your Own Business Act, which not only seeks to introduce new standards for user privacy and how data is handled, but would also impose criminal penalties, including jail time, on the leadership of companies that fail to comply.

Sen. Marco Rubio (R-Fla.) also introduced a privacy-related bill earlier this year. His American Data Dissemination Act would create a process and timeline for the Federal Trade Commission to establish privacy rules, rather than actually establishing new rules. It would also prohibit any state from

enforcing its own law related to the same kinds of data as the federal law, something many big tech companies strongly support.

https://arstechnica.com/?p=1597031