Proposed bill would make monopolies pay “serious” fines



Enlarge / You can’t send corporate “persons” directly to jail, but you can charge them a lot of money.

reader comments

124 with 84 posters participating

Share this story

The Federal Trade Commission’s recent $5 billion settlement with Facebook largely drew two responses. One holds that $5 billion is objectively a large sum of money, while the other holds that, against Facebook’s $55 billion 2018 revenue, the penalty amounts to mere drops in the ocean that will go completely unnoticed within the mammoth company.

Both takes are true: a fine can be both a very large amount of money and yet also not “enough.” The FTC’s ability to penalize businesses, though, is limited under existing law. And so a group of Democratic senators has introduced a bill that could change the law in order to let the FTC fine a bad actor big bucks.

The proposed law basically seeks to deter anticompetitive and monopolistic behavior by charging great gobs of money against the companies that get caught doing it. Businesses found to be in violation of certain antitrust laws would owe the greater of either 15% of their annual US revenue or 30% of all revenue over the period of time the unlawful behavior took place.

Senators Amy Klobuchar (D-Minn.) and Richard Blumenthal (D-Conn.) introduced the bill, which was also cosponsored by senators Dianne Feinstein (D-Calif.) and Ed Markey (D-Mass.).

“We have a major monopoly problem in this country,” Klobuchar said. “Dominant companies need to be put on notice that there will be serious financial consequences for illegal monopolistic behavior.”

Any industry can have companies that abuse their outsized market power, companies that cheat or play unfairly to attain dominance, or companies that squeeze out competition through mergers—the cornerstones of US antitrust law. But here in 2019, “antitrust investigation” seems nearly synonymous with “tech investigation.”

The House in June launched a bipartisan antitrust investigation into big tech. In July, the US Department of Justice confirmed it was working on an antitrust investigation into “search, social media, and some retail services online,” which most folks read to mean Google, Facebook, and Amazon. And in that same week, Facebook said it was the target of an FTC antitrust investigation, separate from the FTC’s probes into its privacy practices.

Months or years will probably go by before those investigations make public any findings. But should this bill defy all current odds and somehow manage to become law, any violations could prove expensive.

https://arstechnica.com/?p=1546075

Cloudflare has had enough, cutting off 8chan



Enlarge / Matthew Prince, co-founder and chief executive officer of CloudFlare Inc.
Bloomberg/Getty Images

reader comments

146 with 90 posters participating

Share this story

In the wake of Saturday's mass shooting in El Paso, in which 20 people lost their lives, it was discovered that the shooter had posted a racist manifesto on the imageboard site 8chan. That was the third time this year alone that a mass shooting has involved the notorious site, and network operator Cloudflare decided that was finally enough. As of midnight on the US West Coast, Cloudflare will cut off 8chan.

This isn't the first time that the popular service provider has severed its ties to one of its customers over offensive content. In 2017, the company dropped the white supremacist website the Daily Stormer. The Daily Stormer was able to get back online after a brief outage by switching to another service.

Matthew Prince, the company's co-founder and CEO, has always spoken with apprehension about whether to stop providing network services to specific websites. He called his own company's decision regarding the Daily Stormer "arbitrary" and "dangerous," and intended that this would be the last action of the sort Cloudflare would take. Earlier on Sunday, CNN reported that the company had no intention of acting against 8chan.

Cloudflare is not a website hosting provider. The company operates a global network that improves performance of websites and protects them from DDoS attacks and other security threats.

But the El Paso mass shooting comes in the wake of two similar manifestos posted to 8chan prior to similar events in California and New Zealand, all apparently prompted by racism. Prince cited both of those events in announcing that he's

changed his mind. “The rationale is simple,” he wrote. “They have proven themselves to be lawless, and that lawlessness has caused multiple tragic deaths.” He went on to state that the company’s guiding principle on this issue will be to disassociate itself from websites that “directly inspire tragic events and are lawless by design.”

He also addressed the fact that many view this as a free speech issue:

> *Some have wrongly speculated this is due to some conception of the United States’ First Amendment. That is incorrect. First, we are a private company and not bound by the First Amendment. Second, the vast majority of our customers, and more than 50% of our revenue, comes from outside the United States where the First Amendment and similarly libertarian freedom of speech protections do not apply.*

Prince acknowledged that 8chan will be able to find another service provider to take over from Cloudflare. While he called on policymakers to clarify what network services can do in response to sites that he views as lawless, that’s going to be a long-term process. For now, Prince acknowledged, “We’ve solved our own problem, but we haven’t solved the Internet’s.”

This article was corrected to clarify that Cloudflare is not a hosting service.

https://arstechnica.com/?p=1545985

Barr says the US needs

encryption backdoors to prevent “going dark.” Um, what?



Enlarge / US Attorney General William Barr speaks at the International Conference on Cyber Security at Fordham University School of Law on July 23, 2019 in New York City. In his remarks, Barr stated that increased encryption of data on phones and encrypted messaging apps puts American security at risk. Barr encouraged technology companies to provide law enforcement with access to encrypted data during certain criminal investigations.
Drew Angerer/Getty Images

reader comments

151 with 121 posters participating, including story author

Share this story

On July 23, in a keynote address at the International Conference on Cyber Security at Fordham University, US Attorney General William Barr took up a banner that the Justice Department and Federal Bureau of Investigation have been waving for over a decade: the call for what former FBI director James Comey had referred to as a "golden key."

Citing the threat posed by violent criminals using encryption to hide their activities from law enforcement, Barr said that information security "should not come at the expense of making us more vulnerable in the real world." He claimed that this is what is happening today.

"Service providers, device manufacturers, and application developers are developing and deploying encryption that can only be decrypted by the end user or customer, and they are refusing to provide technology that allows for lawful access by law enforcement agencies in appropriate circumstances," Barr proclaimed.

And this, he said, was making it increasingly difficult for law enforcement to surveil criminal activity. This blindspot what also allowing criminals to make their information and communications "warrant proof… extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes," and allowing "criminals to operate with impunity, hiding their activities under an impenetrable cloak of secrecy."

In other words, the lawful surveillance capabilities of the government are "going dark," according to AG Barr.

"The net effect is to reduce the overall security of society," he continued. "I am here today to tell you that, as we use encryption to improve cybersecurity, we must ensure that we retain society's ability to gain lawful access to data and communications when needed to respond to criminal

activity.” AG Barr closed by saying that US citizens should accept encryption backdoors because backdoors are essential to our security.

In response, Gen. Michael Hayden, former director of the National Security Agency, said, “Not really.”

> *Not really. And I was the director of national security agency*
>
> *— Gen Michael Hayden (@GenMhayden) July 23, 2019*

Regardless of the accuracy of Barr’s claims, encryption is certainly far more prevalent than it was even five years ago—back when freshly minted memoirist Edward Snowden gave the world a look at the workings of US intelligence agencies’ digital surveillance capabilities. For better or worse, Snowden’s data dump continues to shake up not just the world’s view of communication privacy—it upended the world’s view of information security in general.

Snowden’s impact on the *de jure* of mass surveillance was perhaps less than he would have hoped for. But his revelations had wide-ranging effects on the tech industry and on the development of Internet and security standards. While Snowden opened up a dialogue about intelligence policy, “some of the most significant reforms were technical, not legal.”

That’s according to Ben Wizner of the American Civil Liberties Union, who has acted as Snowden’s attorney. “The proliferation of encryption was rapidly accelerated,” he says. “And the Internet is more secure today than it was in 2013. Technology companies realized that they had been operating under the wrong threat model.”

After Snowden, Internet and technology firms could no longer ignore the threat posed by state-funded actors to their customers, said Mark Rumold, senior staff attorney at the

Electronic Frontier Foundation (EFF). He went on:

> *Companies recognized guarding against state surveillance is a bottom line issue for them… It is a question of financial interest to these companies to be able to convince their users that their data is secure with them, so we saw a lot of companies take steps to roll out encryption in various ways and I think that there's no question that this enhances security and privacy.*

Just how much those steps have hindered legal surveillance and investigation—attempts by law enforcement and intelligence agencies operating under the authority of a court-approved warrant—is in dispute. As information security professional Robert Graham pointed out in a recent blog post, there is no evidence of a surge in crime corresponding to the use of encryption. Such claims, he says, are "based on emotional anecdotes rather than statistics."

Even allegedly hard data presented by the government has been routinely inflated. In December 2017, FBI Director Christopher Wray claimed in Congressional testimony that, in the 2017 fiscal year, the bureau "was unable to access the content of approximately 7,800 mobile devices" using available tools. Wray made this proclamation a year after the government's highly public battle over encryption with Apple in the wake of the tragedy in San Bernardino, California. But that figure was vastly larger than the 880 devices the FBI had cited a year before, and a Washington Post investigation found that the number of inaccessible devices in 2017 was actually about 1,200 according to an FBI internal estimate.

So, is surveillance really "going dark"? Or is this, as Graham suggested, "a Golden Age of Surveillance" where even more privacy is required? Joseph Lorenzo Hall, Chief Technologist at the Center for Democracy and Technology (CDT), leans toward the latter.

“The FBI says they’re ‘going dark’,” Hall told Ars. “Well yeah, because they’ve been staring at the sun.”

Fixing overexposure



Like this prison in Cuba, the NSA has turned the Internet into a place where the watchmen can see all and exploit the shoddy privacy of Internet services prior to Snowden.

Much of the Internet has become more secure over the past five years. The Snowden revelations may not have directly caused the rise of secure Web protocols, but they sure helped motivate protocol development. While the threat of a “global observer” on the Internet had been theorized before Snowden, his evidence of that sort of capability immediately triggered a response from the technical community.

“The engineering community took the succession of Snowden revelations really seriously,” Hall told Ars. Just 11 months after the first of the leaks, the Internet Engineering Task Force put out RFC 7258, “stating that pervasive monitoring is an attack,” Hall noted.

To be fair, the Internet in 2014 had practically nowhere to go but up in terms of protecting privacy. Almost all of the fundamental building blocks of the Internet were, at the time, "almost completely insecure" since their creation, Hall explained. That's "because we were experimenting with them. And now we're retroactively having to go back and put security back on."

That shift in perception of the threat of mass surveillance was followed by significant improvements in securing Web traffic. That included much more security-focused operations at major Internet service providers. Two particular changes were accelerated by the Snowden revelations: adoption of secure HTTP (HTTPS) and TLS encryption by major Internet services, and the development of Transport Layer Security (TLS) 1.3.

HTTPS has had the biggest effect so far, and the changes in TLS will further close the door on surveillance. In 2013, less than 30% of Web traffic was encrypted, and less than 10% of websites supported secure connections. By 2017, more than half of the Web supported HTTPS, and today over 70% of Web traffic is encrypted, based on data from Google and Let's Encrypt. As of April 2019, 91% of webpages visited by US users were secured. Internationally, about 85% of webpages visited were encrypted.

Adoption of encryption for email traffic—both between client and server and from provider to provider—also grew dramatically as a direct result of the Snowden revelations. In early 2014, only about a quarter of the email traffic between Google and other providers was encrypted. Now, it's over 75%.

The adoption of encryption has had major implications for both the intelligence community and law enforcement, at least in terms of "traditional" Internet traffic. Much of the metadata we examined in our 2014 project with NPR that was usable for surveillance by the NSA's XKeyscore system has become much

less accessible. We re-staged the tests recently, using ourselves as the victim. Many of the identifiers and other content we were able to pick out of passive traffic collection in 2014 have been dramatically reduced. That isn’t to say that they’re gone—they’re just concealed within encrypted HTTPS and TLS traffic now, at least for standard Web and email traffic.

This practical consideration may be directly responsible for NSA dropping “about” collection (searching the contents of traffic for communications that mentions specific keywords or identifiers for persons of interest). But there are still other ways to gather surveillance data from Internet traffic that won’t be going dark anytime soon.

Listing image by Markus Gann / EyeEm via Getty Images

https://arstechnica.com/?p=1400515

Sex tech companies protest for the right to advertise—online or in the subway



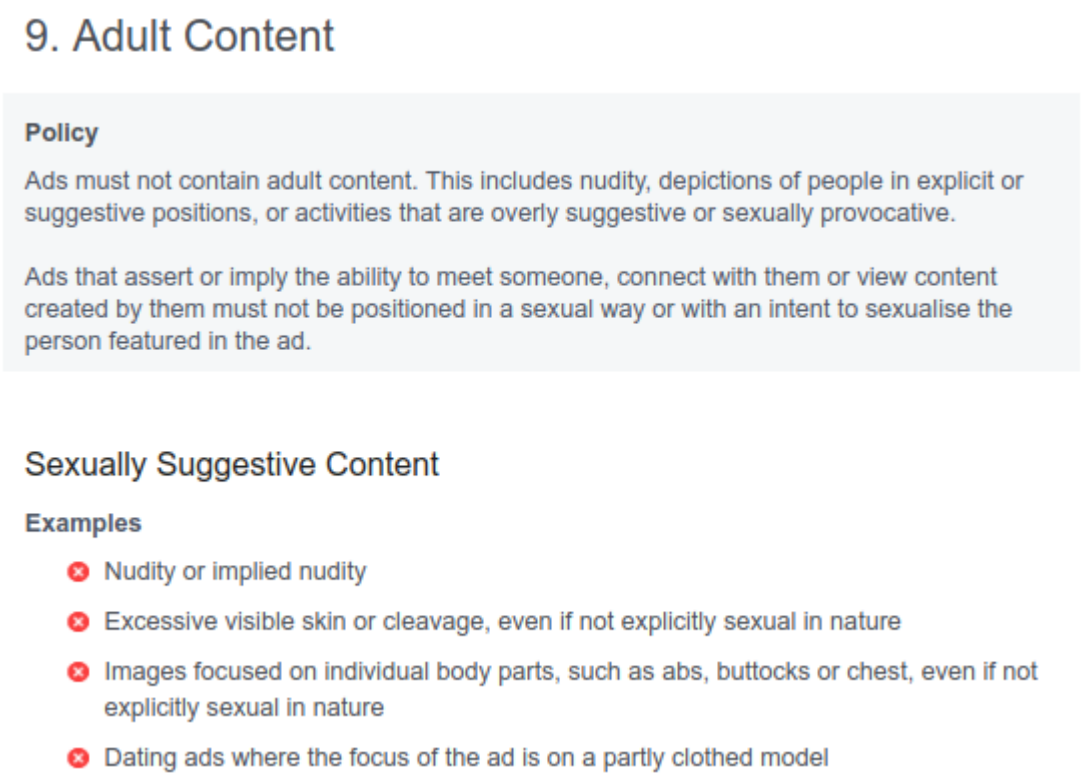
Dame / Unbound

reader comments

95 with 53 posters participating, including story author

Share this story

If you use Facebook heavily, it might come as a surprise that the platform says it prohibits adult content in ads. With everything from a constant stream of “boosted” posts from fitness models to erectile dysfunction ads and “how to initiate sex” ads aimed at brainwashing your wife showing up in timelines, this seems like a weird flex. But Facebook—along with other companies and organizations, like the NYC MTA—does have such a policy. Unfortunately, enforcement of this kind of policy tends to be wink-wink nudge-nudge for ads and services targeting straight male customers, but it’s often enforced sternly by-the-book for everyone else.



This is Facebook's stated policy on adult content in advertisements.

Facebook's policy goes on to provide example images of prohibited content, which revolve in theory around nudity, "implied nudity," and excessive skin/cleavage or focus on a particular body part "even if not explicitly sexual." The problem is not so much with the policy as its uneven enforcement. Ads which clearly violate the stated policy—including but not limited to underwear companies or fitness models with tightly-cropped and suggestive poses, lots of skin, etc—routinely make it through, while ads for female-oriented sexual wellness products or educational posts, seemingly no matter how restrained, are stopped cold. So some companies in the sex tech area have now decided not to take such policy implementation lying down.

- Facebook disapproved this innocuous ad for a Dame handheld vibrator.
- Facebook approved this Manscaped ad—shave 'em if you got 'em, I guess?
- Facebook refused to boost this educational blog post centered around communication and consent.

- Facebook approved this Hims ad featuring a rather self-satisfied model who, one supposes, enjoys his Tadalafil.
- The New York MTA refused to allow this Unbound advertisement in the subway.
- These breast augmentation ads were plastered all over NYC subways.
  approvednotapproved
- This ad for erectile performance enhancements, featuring a very on-the-nose droopy cactus, was approved by the New York MTA.
- This ad for a Dame handheld vibrator was disapproved by the New York MTA.

Approved, not approved

Two woman-owned sexual wellness companies, Unbound and Dame Products, have started a campaign to address this discriminatory policy enforcement. The campaign's website, approvednotapproved, encourages visitors to play a maddening guessing game in which they're shown advertisements and asked to guess whether those ads were allowed. For now, the campaign mostly targets Facebook, Instagram, and the New York MTA (aka, metro or subway ads).

"[I'd like to see] when applicable, advertisers offer an ad category for 'sexual health and wellness' shown only to those 18-plus," Janet Lieberman, CTO of Dame Products, told Ars. "[And I'd like to see] advertisers treat sexual wellness solutions for all sexes and genders equally in how they approve or deny advertisements, without applying their own viewpoint-specific filters on what is or is not wellness."

In addition to the ongoing digital campaign, Dame and Unbound sponsored a protest this week on Facebook's campus. The protest didn't appear heavily attended, but the signage of those who did show up contained clear and direct messaging.

- The homemade signs tended to be more political than the ones provided by Dame/Unbound.
  Dame/Unbound
- Equally important, at any rate…
  Dame/Unbound
- The “ad images” on this protester’s sign aren’t actually ads; they’re Facebook’s example images for what constitutes prohibited “adult content” in advertisement.
  Dame/Unbound
- The homemade signs tended to be a lot more politicized than the ones provided by Dame/Unbound.
  Dame/Unbound
- Despite doing a pretty impressive job of making their ads non-prurient, Dame and Unbound get regularly rejected from platforms like Facebook, Instagram, and the NYC subway.
  Dame/Unbound
- Despite doing a pretty impressive job of making their ads non-prurient, Dame and Unbound get regularly rejected from platforms like Facebook, Instagram, and the NYC subway.
  Dame/Unbound

“We would have no issue with the current content guidelines that most platforms have regarding imagery and language if they were enforced consistently. We simply want the opportunity to direct interested consumers to our products using innocuous creative [ads], on par with or tamer than what they’re already seeing,” Liberman says. “Digital platforms in particular know a lot about who they’re targeting. My ads knew I was getting married before I was even formally engaged. We think it’s about time they use those tools to allow tasteful sexual wellness ads to be shown to the adults who will appreciate them.”

The heart of the two companies’ issue with various advertising boils down to gender bias—presumably unconscious—that unfairly

penalizes advertisements targeted specifically to women. While this is a serious accusation, it shouldn't be particularly surprising or hard-to-believe; studies demonstrating biases that favor men and penalize women are numerous and well-established.

Wait, what's a "sexual wellness company?"

In this article, we refer to both Unbound and Dame Products as sexual wellness companies. There doesn't seem to be a single well-defined and broadly understood word that refers to what they do, which mostly boils down to the manufacturing and sales of sex toys that are designed to be high-quality and body-appropriate, rather than tawdry or shocking. (As Lieberman put it, "ED medications or condoms might be the most relevant products for some, vibrators, lubricants, erotica, or educational materials might be the most impactful solutions for others—that only scratches the surface of the variety of sexual wellness products.")

When we talked to Lieberman—an MIT alumna with experience in mechanical engineering and industrial design—she told us that a large part of the reason she co-founded Dame Products was the lower standard of design and engineering she saw in existing vibrators as compared to other consumer electronics. There was a contrast in the quality and design inherent in mainstream consumer products versus "novelties," which is the category sex toys are typically listed under.

Although the two companies behind the "Approved, Not Approved" campaign clearly differ when it comes to their products' style, both emphasize female-focused ergonomics and design, and they eschew the sort of anthropomorphic (read: it looks like a penis) designs that frequently descend well into the Uncanny Valley.

Ars readers (maybe like the Internet at large) tend to get pretty hot and bothered on both sides of the topic of family-friendly censorship, and we don't expect those partisan reactions to be any different here. Some folks will undoubtedly say we'd all be better off with all the sex in all the places, and a few will probably think *all* of the ad samples above should be banned. Whichever side of that debate you find yourself on, it's worth noting the clear selective bias. As "Approved, Not Approved" indicates, sexual content seems to be getting filtered or approved not on the basis of how tacky or tasteful, educational or pandering it is, but on whether or not it appeals to men.

https://arstechnica.com/?p=1544283

Navy pilot dead after crash in "Star Wars Canyon" in Death Valley [Updated]



Enlarge / An F/A-18 from VFA-151, “the Vigilantes.” A similar aircraft from the squadron crashed on Wednesday flying through what aviation enthusiasts refer to as “Star Wars Canyon” in Death Valley, California.
VFA-151, US Navy

reader comments

103 with 60 posters participating

Share this story

The US Navy has confirmed the death of a pilot in the crash of a Boeing F/A-18E Super Hornet in Death Valley National Park in California on Wednesday. The pilot, who has not yet been named, apparently crashed into the wall of what is known as “Star Wars Canyon”—an area frequently used by the Navy and other services for low-altitude flight training, adjacent to the Naval Air Weapons Station at China Lake. The area, called “Jedi Transition” by the military, is open to the public and is a hotspot for military aircraft photographers and

enthusiasts because of how close aircraft pass when traversing the area. Seven onlookers suffered minor injuries as a result of the crash.

The Navy is waiting for notification of family members before releasing the pilot's name. Navy spokeswoman Lieutenant Commander Lydia Bock said in a press statement that the aircraft—from Strike Fighter Squadron (VFA) 151 ("the Vigilantes"), out of Naval Air Station Lemoore in California—crashed at about 10am PST on Wednesday. "The cause of the crash is under investigation," Bock said. At the time of the initial release, the status of the pilot was unknown, and search and rescue personnel were at the scene.

[Update, 5:32 PM] The Navy has now identified the pilot as Lt. Charles Z. Walker, 33. "The NAS Lemoore aviation family is grieving the loss of one of our own," Capt. James Bates, Commander of Strike Fighter Wing Pacific said in a statement. "Lt. Walker was an incredible naval aviator, husband and son. He was an integral member of the Vigilante family, and his absence will be keenly felt on this flight line. Our aviators understand the risk associated with this profession, and they knowingly accept it in service to our nation. The untimely loss of a fellow aviator and shipmate pains us all. Our heartfelt condolences go out to his family and friends."

Star Wars Canyon, so named because of its proximity to an area used as the location for filming scenes on the fictional planet Tatooine in the original *Star Wars* film, has been used for low-level flight training by the services since the 1930s. When Death Valley became a national park in 1994, the military was given a waiver to continue to use the area for flight training. In 2010, the National Park Service installed railings along the canyon because of the popularity of the location for plane-watching. Like the Mach Loop in Wales, it is one of the few places where photographers can routinely take pictures of military aircraft from *above* as they fly past.



Enlarge / An F-117 Nighthawk Stealth Fighter flies near the “Jedi Transition” on February 27, 2019 in Death Valley, California.
Jerod Harris / Getty Images
[embedded content]
Video of aircraft flying through “Star Wars Canyon”
Witnesses said that the F/A-18 crashed at high-speed directly into a canyon wall. The aircraft exploded in a fireball, scorching the rocks. The pilot never ejected.

VF-151 is part of Carrier Air Wing 9, the air group that recently returned from deployment aboard the USS *John C. Stennis* (CVN-74). The *Stennis* is now in Norfolk after an around-the-world deployment, preparing for mid-life refueling of its nuclear reactors.

https://arstechnica.com/?p=1545413

Domino’s takes its case for non-accessible design to the Supreme Court



Enlarge / Visually impaired consumers use screen readers, special input devices, and other technologies to access the internet—at least, on sites designed to accommodate it.

reader comments

268 with 128 posters participating

Share this story

The shift toward using an app on your phone to place an order, instead of using your phone to call a place, has made life easier for millions of people. Unfortunately, that shift has the opposite effect on blind and visually impaired consumers, for whom thousands of websites and mobile apps are unusable.

Domino’s Pizza maintains one such site, and it’s asking the Supreme Court to let the site stay that way.

Domino’s made a legal filing called a writ of certiorari to the US Supreme Court last week—basically, an argument for why the nation’s highest court should take its case. In the petition (PDF), Domino’s asks the court to determine whether the Americans with Disabilities Act (ADA) requires a retailer’s website or app to “satisfy discrete accessibility requirements with respect to individuals with disabilities.”

“Websites and mobile apps do not become public accommodations simply by virtue of providing access to the goods and services of a brick-and-mortar enterprise,” the pizza chain argues. The ADA “does not demand full accessibility for each and every means of accessing the goods or services a public accommodation provides to the public.”

As courts have split on the digital accessibility issue several times in the past two decades, Domino’s said, the time is “ripe” for Supreme Court intervention.

The background

A blind consumer in California tried at least twice to order a pizza from Domino’s using its website and app, but the customer was unable to complete the transaction because Domino’s services were not designed to be accessible to the blind. In 2016, he filed suit against the pizza delivery chain, alleging a violation of the ADA.

The district court dismissed his case, so he appealed. The Ninth Circuit Court of Appeals heard the case last year and ruled in the customer’s favor in January of this year.

In that ruling (PDF), the appellate court determined that “the ADA applied to Domino’s website and app because the Act mandates that places of public accommodation, like Domino’s,

provide auxiliary aids and services to make visual materials available to individuals who are blind.”

In its appeal to the Supreme Court, Domino’s claims the Ninth Circuit ruling is flat-out “wrong” and needs to be addressed before businesses spend time and money adapting their digital storefronts to meet “unclear and shifting standards.”

The legal question

Parties on both sides of this and several previous lawsuits have pointed out that the law itself is unclear. The ADA doesn’t have any specific provisions dealing with Web or mobile storefronts because it became law in the long-ago era of 1990, before such services existed.

Title III of the Act, however, is devoted to “public accommodations and services operated by private entities,” including retailers and restaurants. Most brick-and-mortar venues, with some specific exceptions, are required to make reasonable accommodations for customers with disabilities, such as keeping aisles a certain minimum width, installing ramps or elevators, adding braille or raised print to certain signs, or allowing service animals.

ADA compliance and enforcement is far from perfect in physical spaces, but at least the law exists. But courts are indeed badly split over whether digital spaces—rapidly becoming a dominant sector of the US economy—also fall under Title III protections.

The Justice Department has changed its position on the question several times in the intervening decades, but it never actually issued a final rule or a unified guidance either way, leaving the matter to be handled in court.

Accessibility technology firm UsableNet said in a recent report that more than 2,200 lawsuits related to Web

accessibility issues were filed nationwide in 2018, with a combined 49 percent of those suits filed against retail and food service businesses.

These suits are a “no-win scenario” for companies on the receiving end, Domino’s said. “And it is also a no-win scenario for individuals with disabilities, because defendants faced with these suits overwhelmingly enter into piecemeal monetary settlements with individual plaintiffs or eliminate their online offerings instead of trying to keep up with moving-target compliance standards” that evolve as technology changes.

In its petition, Domino’s cites cases decided by the First, Second, and Seventh Circuits all determining that businesses that only operate in the digital sphere are subject to Title III liability—and cases decided by the Third, Sixth, and Ninth Circuits determining that they are not.

This wave of lawsuits means time is of the essence, Domino’s wrote in its filing. “This case is an ideal vehicle for the Court to address whether and how Title III applies to websites, and that issue need not percolate any further,” Domino’s said. “Courts have thoroughly aired the competing arguments over whether Title III applies to the internet, and have chosen their sides.”

https://arstechnica.com/?p=1545319

Apple and Google temporarily

stop listening to Siri and OK Google queries



Enlarge / An Apple Watch Nike+ Series 4.
Getty Images | Wachiwit

reader comments

79 with 50 posters participating

Share this story

Apple workers have stopped listening to Siri queries worldwide, the company said this week. Apple plans to bring back human reviews of Siri voice recordings at some unspecified date, but the company said it will only review them when customers specifically opt in to the practice.

Separately, Google today confirmed that it recently “paused” human reviews of Google Assistant queries worldwide.

Apple’s decision to stop having humans listen to Siri queries follows a report last week that contractors who review the recordings for accuracy heard private discussions and even sexual encounters.

Apple calls the human reviews of Siri recordings “grading.”

“We are committed to delivering a great Siri experience while protecting user privacy,” Apple told Ars and other news organizations. “While we conduct a thorough review, we are suspending Siri grading globally. Additionally, as part of a future software update, users will have the ability to choose to participate in grading.”

Apple had no further comment, a spokesperson said.

Google “paused reviews globally”

A German investigation into Google began after a Google contractor leaked 1,000 voice recordings to VRT NWS, a news organization run by a public broadcaster in the Flemish region of Belgium. VRT NWS reviewed the recordings and was able to identify some of the people who were recorded. VRT NWS also said that 153 of the 1,000 recordings it listened to “were conversations that should never have been recorded and during which the command ‘OK Google’ was clearly not given.”

“Shortly after we learned about the leaking of confidential Dutch audio data, we paused language reviews of the Assistant to investigate. This paused reviews globally,” Google told Ars today.

Google previously told Ars that “You must opt in to have your audio recordings stored to your account, and Voice and Audio Activity is not required to use the Google Assistant.”

“You can turn off storing audio data to your Google account completely, or choose to auto-delete data after every three months or 18 months,” the company noted today. The ability to

turn off storage of voice activity can be found in Google activity controls.

Google didn’t say when it will resume human reviews of Google Assistant recordings. However, Google was ordered by German authorities to stop human evaluations of Google Assistant queries for at least three months.

Google confirmed to those authorities “that transcriptions of voice recordings will no longer be carried out at present and for at least three months from 1 August 2019,” according to the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI). This covers all recordings in the European Union, the agency said.

The three-month ban “is intended to provisionally protect the rights of privacy of data subjects for the time being,” while data protection authorities investigate and consider a more permanent solution, the HmbBfDI said.

Apple stores voice recordings

As The Verge noted, Apple’s new statement did not say whether it will stop storing Siri voice recordings on its servers. “Currently the company says it keeps recordings for six months before removing identifying information from a copy that it could keep for two years or more,” The Verge report said.

Apple told The Guardian last week that it has humans review “a small portion” of Siri requests “to improve Siri and dictation.”

“User requests are not associated with the user’s Apple ID,” Apple also said. “Siri responses are analyzed in secure facilities and all reviewers are under the obligation to adhere to Apple’s strict confidentiality requirements.” Fewer than 1% of Siri recordings are analyzed by humans, and “those used are typically only a few seconds long,” Apple also told

the newspaper.

Amazon also has humans reviewing Alexa recordings, which are stored indefinitely unless customers delete them. We asked Amazon today if it is stopping the voice reviews, and we'll update this article if we get a response.

https://arstechnica.com/?p=1545149

Pai's FCC orders cities and towns to stop regulating cable broadband



Enlarge / FCC Chairman Ajit Pai on December 14, 2017, in Washington, DC, the day of the FCC's vote to repeal net

neutrality rules.

reader comments

76 with 62 posters participating

Share this story

The Federal Communications Commission today ordered cities and towns across the country to stop regulating broadband delivered over cable networks.

The vote to approve Chairman Ajit Pai's plan also limits the fees that municipalities can charge cable companies. This could impact public TV stations and services that network operators provide cities and towns in exchange for cable TV franchises.

The FCC announcement of its decision said, "the Order prohibits excessive franchise fees and explains that local governments may not regulate most non-cable services, including broadband Internet access service, offered over a cable system." The FCC claimed that its decision "remove[s] obstacles to the deployment of broadband."

Cities and towns object

Many cities and towns had written to the FCC urging it to scrap the plan.

"We've heard from thousands of communities across the country worried we are cutting the operations of so many local channels," FCC Commissioner Jessica Rosenworcel, a Democrat, said while voting against Pai's plan. "I am saddened that this agency refuses to listen."

The FCC's Republican majority "insist[s] that funding these local stations and related efforts damages the ability of our nation's broadband providers to extend their networks to

communities without high-speed service," Rosenworcel said. But ISPs haven't actually promised to deploy more broadband in exchange for the regulatory favor from the FCC, she said.

"Comb through the text of this decision," Rosenworcel said. "You will not find a single commitment made to providing more broadband service in remote communities. There is no enforceable obligation to expand broadband capacity. There is no agreement that any savings from today's action is pushed into new network deployment. I fear this absence speaks volumes."

Pai's FCC has repeatedly claimed the authority to preempt local regulation of broadband despite the FCC abandoning its own Title II authority to regulate broadband.

Today's vote "is consistent with the commission's current perplexing view that it has no statutory authority over broadband but can nevertheless preempt states and local authorities from exercising their own authority," said John Bergmayer, legal director of consumer advocacy group Public Knowledge.

The FCC is likely to face a lawsuit over today's decision. Bergmayer predicted that the FCC order will be overturned.

"In this case the commission has decided to pursue a theory that an obscure provision of Title VI of the Communications Act gives it broad powers to substitute its views for those of local governments that are closer to the people they serve," he said. "We're confident that this unreasonable exercise in statutory gymnastics will eventually be rejected." The FCC decision "contradicts numerous federal and state courts that have read the statute and found it contains no such broad preemption authority," Bergmayer also said.

Comcast case helped spur FCC action

Pai's proposal complained that "some states and localities are purporting to assert authority" to collect fees and impose requirements that aren't explicitly allowed by Title VI, the cable-regulation section that Congress added to communications law with the Cable Act of 1984.

US cable law prevents local authorities from collecting more than 5% of a cable operator's gross revenue in any 12-month period. In today's announcement, Pai's office said some local governments have been requiring in-kind contributions from cable operators to get around the 5% cap and that the FCC preemption will "rein in [this] overreach by local franchising authorities." The FCC order says that most in-kind contributions must count toward the 5% cap.

The FCC action was spurred partly by an Oregon state Supreme Court decision that upheld a 7% "telecommunications" license fee the city of Eugene imposed on Comcast. The FCC's Republican majority says the court got the law wrong.

Republican FCC Commissioner Michael O'Rielly said:

> *Inappropriate court determinations, such as the Eugene, Oregon, franchise case have wrongly tried to open the door to the imposition of such fees on other services offered by what have traditionally been called cable operators. However, the statute is quite clear on the matter and the item appropriately clarifies that franchise authorities can only regulate cable services. Today's action closes off potential revenues for franchise authorities from non-cable services, which is the right statutory reading.*

“Grave harm to local communities”

The FCC vote was 3-2, with dissents from Rosenworcel and Geoffrey Starks, the FCC’s other Democrat.

Starks said:

> *Thousands of federal, state, and local leaders have submitted substantive comments in our docket, pointing out how our action today will… target certain terms negotiated into franchise agreements that are of great importance to local communities. From free or discounted services to schools or government buildings, to institutional networks, or I-Nets, which are viewed as critical infrastructure by many cities and relied upon to support government functions and public safety communications, much is at stake.*

Public, educational, and governmental (PEG) channels that are funded by franchise agreements will also take a hit, he said. “Free or discounted service to cash-strapped schools, provision of critical I-Nets, discounts to vulnerable communities—all of these franchise terms advance the public interest and are a small imposition given the value received by providers in franchise negotiations,” Starks said. “Our action today is unnecessary, unsupported by law or precedent, and risks causing grave harm to local communities.”

Pai defended the order by saying that fees charged by local authorities get passed on to consumers by cable companies. He said:

> *Every dollar paid in excessive fees is by definition a dollar that cannot and will not be invested in upgrading and expanding networks… This discourages the deployment of new services, like faster home broadband or better Wi-Fi or Internet-of-things networks. By simply insisting that LFAs [local franchising authorities] comply with the law, we will*

reduce costs for consumers and expedite the deployment of next-generation services.

https://arstechnica.com/?p=1544797

FBI says “extremists” motivated by Pizzagate, QAnon are threats



Enlarge / The seal of the Federal Bureau of Investigation (FBI) hangs on a wall before a news conference at the FBI headquarters in Washington, DC, on Thursday, June 14, 2018.

reader comments

194 with 105 posters participating

Share this story

The modern era of the Internet has given us a seemingly never-ending bounty of farfetched conspiracy theories. Some of the loudest of those fringe movements have become pervasive enough and serious enough to qualify as domestic terror threats, the FBI says.

Yahoo News today published an internal FBI document it obtained warning of "conspiracy-theory-driven domestic extremists."

The memo, dated May 30, describes "anti-government, identity-based, and fringe political conspiracy theories" as likely to motivate extremists "to commit criminal or violent activity."

In the memo, the FBI says the document is the first bureau product to explicitly discuss the future threat from domestic extremists driven by modern conspiracy theories.

Conspiracy theories of some kind or another are nearly as old as communication itself, but the always-online era has accelerated their growth and broadened their spread.

"Although conspiracy theory-driven crime and violence is not a new phenomenon," the memo continues, "Today's information environment has changed the way conspiracy theories develop, spread, and evolve."

In the FBI's assessment, the bureau warns, these conspiracy movements "very likely will emerge, spread, and evolve in the modern information marketplace over the near term, fostering anti-government sentiment, promoting racial and religious prejudice, increasing political tensions, and occasionally driving both groups and individuals to commit criminal or

violent acts," especially as we move into the 2020 election season.

The FBI, later in the document, defines "very likely" as a greater than 80% chance of something occurring.

Not just a hypothetical

The memo explicitly cites both Pizzagate and QAnon as examples of modern "fringe political" conspiracy theories that have already been implicated in violence.

The "Pizzagate" theory came to a head in 2016, when a devotee marched into a DC pizzeria with an AR-15 and started making threats.

The theory claimed—falsely—that high-ranking Democratic Party officials were operating a child sex ring out of the basement of the pizza shop, which received hundreds of threats. The shooter took it upon himself to "self-investigate" and was ultimately sentenced to four years in prison on weapons and assault charges.

The assault on the pizzeria did not stop the conspiracists. As recently as December, the FBI memo says, an individual found in possession of bomb-making materials said he was going to blow up a monument in Springfield, Illinois, "to make Americans aware of Pizzagate" and other conspiracies.

QAnon, meanwhile, is complicated enough that its own adherents can sometimes barely follow all its ins and outs. In broad strokes, QAnon posits that an anonymous insider known as "Q" is constantly dripping out insider information about Donald Trump's byzantine, long-term plans to take down the "deep state."

Although still a fringe belief, some right-wing celebrities and pundits have embraced the conspiracy and lent more credence to its followers. These enthusiasts subsequently show

up at Trump rallies and draw positive attention from the president.

In June 2018, a Nevada man used an armored truck to block all traffic next to the Hoover Dam. The man, who was found to have several weapons inside his vehicle, “referenced the QAnon conspiracy theory directly and discussed related conspiratorial beliefs after his arrest,” the FBI memo says.

That incident came only a few weeks after a different man claimed a homeless camp in Arizona was actually the site of child trafficking. After law enforcement came to investigate and found nothing, he “repeatedly alleged a law enforcement cover-up and referenced the QAnon conspiracy theory as he and armed group members searched for additional camps” and engaged in “criminal activities,” according to the memo.

A former Department of Homeland Security counterterrorism official told Yahoo News that while the threat may be real, it seems unlikely to be mitigated any time soon. “Nearly all, if not all, the intelligence analysts focusing on domestic extremist groups” at DHS have left or been put out of work during the Trump administration, he told Yahoo. “There is no one there” to do the work to investigate or stop it.

The FBI, for its part, told Yahoo News in a statement that it can “never initiate an investigation based solely on First Amendment protected activity. As with all of our investigations, the FBI can never monitor a website or a social media platform without probable cause.”

Another right-wing conspiracy theory, related to the 2016 killing of Democratic National Committee staffer Seth Rich, was recently reported to be the work of Russian intelligence.

https://arstechnica.com/?p=1544539

TV networks sue nonprofit to kill free TV service



Getty Images | Jacobo Zanella

reader comments

114 with 84 posters participating

Share this story

The major broadcast networks today sued the makers of Locast, a nonprofit organization that provides free online access to broadcast TV stations. The lawsuit filed by ABC, CBS, Fox, and NBC seeks financial damages and a permanent injunction that would shut Locast down.

Broadcast TV networks are available for free over the air with an antenna. But selling the rights to retransmit those signals in other ways is a big business. Broadcasters reportedly collected $10.1 billion in 2018 via retransmission fees they charge cable and satellite TV companies.

TV providers routinely pass this cost along to consumers in the form of “Broadcast TV” fees. Pay-TV providers use these fees to raise the actual cost of service above their advertised prices and to raise customers’ prices even while they’re under contract.

Pay-TV providers have also been refusing broadcasters’ demands to pay even higher fees, and broadcast channels have frequently been blacked out on cable and satellite TV systems as a result.

Use an antenna—or Locast

TV subscribers can deal with blackouts by using an antenna—or a service like Locast. While Locast is a nonprofit, the broadcasters argue that it’s actually bankrolled by the satellite TV industry. DirecTV owner AT&T notably donated $500,000 to Locast, and Locast’s founder has ties to Dish Network.

Locast says it is on a mission to help TV viewers get easier access to channels that are supposed to be free:

> *Ever since the dawn of TV broadcasting in the mid-20th Century, non-profit organizations have provided “translator” TV stations as a public service. Where a primary broadcaster cannot reach a receiver with a strong enough signal, the translator amplifies that signal with another transmitter, allowing consumers who otherwise could not get the over-the-air signal to receive important programming, including local news, weather and of course, sports. Locast.org provides the same public service, except instead of an over-the-air signal*

> *transmitter, we provide the local broadcast signal via online streaming.*

So far, Locast is available in 13 US markets, namely Baltimore; Boston; Chicago; Dallas; Denver; Houston; Philadelphia; Rapid City, South Dakota; Los Angeles; New York City; San Francisco; Sioux Falls, South Dakota; and Washington, DC. Locast intends to expand to new markets but solicits donations because it says it has "considerable costs for equipment, bandwidth, and operational support." Locast can be used on mobile devices, streaming boxes, and Web browsers; it detects your location and lets you choose from a selection of local TV channels.

Networks claim Locast isn't really a nonprofit

Broadcasters fear that wider availability of free TV channels will make it harder to charge retransmission fees to cable and satellite companies. The networks filed their lawsuit in US District Court for the Southern District of New York against Sports Fans Coalition founder David Goodfriend and the New York chapter of his group, which created Locast. Goodfriend, an attorney and lobbyist, has been fighting TV blackouts for years on multiple fronts.

The lawsuit filed by ABC, CBS, Fox, and NBC says:

> *Plaintiffs, including their affiliated companies, collectively invest billions of dollars to create, acquire, and provide valuable television programming. That programming is broadcast to the public for free over-the-air viewing, but the overwhelming majority of households have elected the convenience and reliability of viewing Plaintiffs' copyrighted programming through services offered by cable, satellite, broadband, and mobile providers. By virtue of*

> *several Acts of Congress, those providers must have a license to retransmit copyrighted television programming, notwithstanding that the programming is broadcast over the air by Plaintiffs and their local affiliates, and must also secure the consent of the broadcasters to retransmit the broadcast signals.*

Even though the TV channels are available for free, Locast can't retransmit them, the lawsuit said:

> *Locast captures over-the-air broadcast signals, strips critical data from those signals, and then retransmits those signals, and the copyrighted content that they carry, to registered users over the Internet. The catch is, unlike licensed cable, satellite, and streaming services, Locast neither obtains Plaintiffs' permission nor pays for its exploitation of Plaintiffs' exclusive rights to publicly perform their copyrighted content. Instead, Locast simply takes Plaintiffs' copyrighted content and retransmits it to its registered users at will over the Internet.*

The broadcasters acknowledged that a 1976 copyright law allows nonprofits to boost local broadcast signals. But they argue that "Locast is nothing like the local booster services contemplated by Congress in creating this narrow exemption." In reality, the networks' lawsuit says that "Locast's founding, funding, and operations reveal its decidedly commercial purposes."

To prove that Locast has "commercial purposes," the lawsuit points to AT&T's $500,000 donation and the fact that Goodfriend is a paid lobbyist for Dish. AT&T and Dish have both fought broadcasters over retransmission fees, leading to blackouts.

The lawsuit says:

> *These two for-profit businesses [AT&T and Dish] provide Locast with valuable nationwide distribution of the Locast app on the Internet-connected set-top boxes of their subscribers. At the same time, Locast provides these two major distributors with commercial benefits that include the ability (a) to avoid obtaining retransmission consent from local stations to include local stations in their pay-TV offerings by integrating the Locast app into their customers' set-top boxes; (b) to gain leverage in negotiations with broadcast stations over retransmission consent rights to offer their subscribers access to broadcast channels; and (c) for Dish, to promote a version of its Sling TV Internet television service that does not carry local broadcast channels by telling potential customers that they can "supplement" Sling TV by getting the broadcast channels via Locast. Locast is not the noncommercial, community public service it purports to be. It is a strategic play funded by and functioning for the benefit of decidedly commercial interests.*

AT&T released a statement saying that "Locast offers consumers an innovative new way to access free over-the-air signals. We support technologies that give consumers more choices and better access to this local content."

Founder ready for legal fight

Will that argument convince a judge or jury? Goodfriend was eager to find out even before he got sued, according to a New York Times article in January titled "Locast, a Free App Streaming Network TV, Would Love to Get Sued."

"I ask people all the time, 'Do you know you're supposed to get television for free?'" Goodfriend said, according to the Times. With Locast, "We are operating under parameters that are designed to be compliant within the law," he also said.

Goodfriend also told the Times that he tried to get funding from Dish Chairman Charlie Ergen but wasn't able to. Goodfriend wasn't drawing a salary from Locast and had taken out a loan to fund the operation, which cost more than $700,000 as of January, the Times article said. AT&T's donation came several months later.

We contacted Goodfriend about the lawsuit today and will update this story if we get a response.

Colorado Law professor Blake Reid thinks the broadcasters' lawsuit has some holes.

"The broadcasters are in a bind here because they could have argued that Locast is a cable system, but they pushed to shoot down that argument back when Aereo made it after losing on fair use in the Supreme Court," Reid told Ars today. "Basically, they want to have their cake and eat it, too—they don't want an Internet-based system to be able to pay for retransmission as a cable system, but that opens up [the possibility] that a non-profit organization like Locast can be eligible for this exemption."

Proving that Locast violates the copyright law's nonprofit exemption will be hard, but maybe not impossible, Reid said.

"The complaint makes some extremely incoherent arguments about Locast somehow gaining commercial advantage as a non-profit," Reid said.

Still, Reid wouldn't rule out the chance of broadcasters succeeding in their argument that Locast's ties to AT&T and Dish undermine its nonprofit status. But winning on that point could be a Pyrrhic victory because it wouldn't stop future services from providing the same service Locast does.

Locast's funding is "a complicated factual issue that I'm not sure we know all the facts about yet, but the best that does for the broadcasters is stop Locast specifically and create a

blueprint for another nonprofit to step up and do the same thing," Reid said.

Aside from the funding question, the plain language of the statute seems to support a nonprofit retransmitting TV signals over the Internet, Reid said. The nonprofit exemption says, "The secondary transmission of a performance or display of a work embodied in a primary transmission is not an infringement of copyright if… the secondary transmission is not made by a cable system but is made by a governmental body, or other nonprofit organization."

To qualify for that exemption, the law says an organization must not have "any purpose of direct or indirect commercial advantage." The broadcasters' argument that Locast is basically a front for AT&T and Dish would thus be a problem for Locast if it can't provide a convincing counter-argument.

But other parts of the statute are probably easy for Locast to satisfy, Reid said. The statute says retransmissions must be made "without charge to the recipients of the secondary transmission other than assessments necessary to defray the actual and reasonable costs of maintaining and operating the secondary transmission service." While Locast solicits donations, it isn't charging users for its service, and so it wouldn't run afoul of that provision.

"This part's very easy for Locast to satisfy as a nonprofit," Reid said.

Locast isn't the only threat to broadcast networks' retransmission fees. A bipartisan bill filed in the House last week seeks to end the current retransmission consent system and "allow free-market contract negotiations to happen under traditional copyright law."

https://arstechnica.com/?p=1544045