GirlsDoPorn, on trial for fraud, still isn’t leveling with new models

reader comments

56 with 42 posters participating

Share this story

In August, we wrote about a group of 22 models who sued the owners of the porn site GirlsDoPorn for fraud. The models say the company told them that pornographic videos of them would only be distributed on DVDs outside the United States. Instead, the videos were published by GirlsDoPorn, a site with plenty of American viewers.

Bianca Bruno, a reporter for Court House News, has been producing invaluable day-by-day coverage of the ongoing trial in San Diego. On Wednesday, the court heard from Matthew Wolfe, a GirlsDoPorn associate who handles day-to-day operations on the site. Wolfe said that GirlsDoPorn is still trying to recruit new models—and it’s still not giving new recruits the full story about how the videos will be used.

When asked whether the contracts signed by new models mention GirlsDoPorn, Wolfe responded, “No, I don’t believe so.” In fact, he admits that the contracts don’t mention any websites at all. He said that if models asked where the videos would be published, he would say the videos would go online but wouldn’t mention a specific site.

Wolfe said most prospective models “didn’t ask” where their

videos would appear. Wolfe confirmed that videos shot by the company were never published on DVD.

If site owners are now telling models that videos will go online, that’s an improvement from the behavior alleged by plaintiffs. The models say they were told videos would never be posted on the Internet.

“If I had known that they were posting it on the Internet, that my name would be attached to it, that it would be in the United States, if I had known that it was more than 30 minutes of filming, if I had known any of that, just any one of those, I wouldn’t have done it,” one of the victims testified in court in August.

After her video appeared online, she texted a woman who had helped recruit her to shoot the video.

“Hey, you lied to me, and they lied to me,” she wrote in a text message. “It’s on a website now and my whole town back home knows. This ruined my life.”

The principal owner of GirlsDoPorn, Michael Pratt, apparently left the United States last month.

“We have been informed that [Pratt] is no longer in the jurisdiction and is no longer available to testify, even though he is under court order” to appear in court, an attorney for the 22 plaintiffs said in mid-September.

https://arstechnica.com/?p=1579435

EU nations can force Facebook to remove content worldwide, court rules

Enlarge / A Facebook logo in front of an EU flag in this photo illustration on November 20, 2017.

reader comments

130 with 82 posters participating

Share this story

Europe’s highest court issued a controversial ruling Thursday with the potential to have staggeringly large implications worldwide. The Court of Justice of the European Union held that Facebook and other social platforms are not only obligated to proactively identify unlawful content but also to block it worldwide if a single country’s authorities demand it.

The ruling (PDF) stems from a case that began in Austria three years ago. A Facebook user posted comments about an Austrian politician, Eva Glawischnig-Piesczek, that Austrian courts found to be illegally defamatory. Glawischnig-Piesczek in 2016 wrote to Facebook Ireland, the company’s EU headquarters, asking the company to delete the comments and limit access to them globally. Facebook refused, Glawischnig-Piesczek sued, and the results of the years of legal wrangling are out today.

A service is not liable for information it’s hosting “if it has no knowledge of its illegal nature or if it acts expeditiously to remove or disable access” to the illegal content as soon as it becomes aware of it, the court said; the

United States operates under a similar standard. The EU's directive on electronic commerce also "prohibits any requirement for the host provider," meaning a company such as Facebook, "to monitor generally information which it stores or to seek actively facts or circumstances indicating illegal activity," the court said.

But that directive does *not* preclude an EU member nation from ordering a service to remove or block access to content that is identical or equivalent to content that has been deemed unlawful in the past, the court ruled. Nations can require, the court said, the use of automated technologies and filters to make it happen. Crucially, the directive also does not prohibit EU member nations from requiring platforms to remove or block access to such information *worldwide*, "within the framework of the relevant international law."

The globe-spanning ruling is the opposite approach the court took less than two weeks ago in a different case, when it held that the so-called right to be forgotten under EU law does not require Google to make certain information inaccessible to the world beyond European borders.

Billions and billions…

There are about 2.4 billion Facebook users worldwide in all but three countries. About 385 million Facebook users are in Europe. The EU's ruling gives outsized power to the body's 28 member states to set the terms of access and limit content for the other 2 billion Facebook users in the world, Facebook said.

The ruling "raises critical questions around freedom of expression and the role that Internet companies should play in monitoring, interpreting, and removing speech that might be illegal in any particular country," Facebook said in a written statement. "It undermines the longstanding principle that one country does not have the right to impose its laws on speech

on another country."

The devil will also be in the details, Facebook noted. "In order to get this right, national courts will have to set out very clear definitions on what 'identical' and 'equivalent' means in practice. We hope the courts take a proportionate and measured approach, to avoid having a chilling effect on freedom of expression."

The ruling casts a fairly broad net over "equivalent" content. It finds that illegality does not necessarily refer to a specific phrase or sentence but rather "information conveying a message the content of which remains essentially unchanged." So content "essentially conveying the same message" but "worded slightly differently, because of the words used or their combination," as compared to the content that was initially deemed illegal, would have to come down.

"Filters can't understand context"

Daphne Keller of Stanford's Center for Internet and Society published a white paper (PDF) in September analyzing the potential outcomes from such a ruling.

Aside from the glaring issue that speech and defamation laws vary wildly from one nation to another, the ruling "will indirectly but seriously affect Internet users' rights, including rights to privacy and freedom of expression and information," Keller wrote. As opponents noted, she added, "filters can't understand context. That means if text, images, or videos violate the law in one situation, filters will likely also block the same material in lawful uses like parody, journalism, or scholarship.

"Laws that let courts in one country reach across borders to take down expression protected in another, or laws that lead tech companies to erect digital borders, have consequences for everything from foreign relations to competition and trade,"

Keller observed.

https://arstechnica.com/?p=1579333

Facebook, Reddit, and others need a deepfakes plan now, senators say

Enlarge / A comparison of an original and deepfake video of Facebook CEO Mark Zuckerberg.

reader comments

87 with 69 posters participating

Share this story

With only 13 months left to go in the seemingly interminable 2020 US election season, senators are calling on Facebook, Snapchat, Reddit, and other social networks to do something sooner, rather than later, about the potential proliferation of misleading “deepfake” videos

“Over two-thirds of Americans now get their news from social media sites,” Sens. Mark Warner (D-Va.) and Marco Rubio (R-Fla.) jointly write in a series of letters to several technology platforms. “Increased reliance on social media will require your company to assume a heightened set of obligations to safeguard the public interest and the public’s trust.”

Image manipulation is nothing new, and doctored and misleading images have frequently gone viral online since enough Americans had fast-enough Internet access to make the sharing of digital images possible. The potential for not only doctored but completely fabricated video to be able to pass for the real thing, however, is a newer trend.

“We believe it is vital that your organization have plans in place to address the attempted use” of technologies that use “machine learning and data analytics techniques” to generate misleading audio or video, the senators said. “Having a clear policy in place for authenticating media, and slowing the pace at which disinformation spreads, can help blunt some of these risks.

To that end, the senators want platforms to tell them, first of all, what their current policies and rules regarding “misleading, synthetic, or fabricated media” are, if such rules even exist. The senators also want to know what recourse victims of fake videos have with the platforms and if the companies even have available to them the technical ability to detect deepfake video.

Rubio and Warner sent similar letters, with the same set of seven questions, to 11 video-sharing platforms: Facebook, Imgur, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitch, Twitter, and YouTube.

Are deepfakes a big problem?

Deepfake video can be identified—if you know how and where to look. But while individual users may be wising up to the clear tells of a badly Photoshopped still image, the general public is not yet adept at parsing fabricated video (and given how often clear hoaxes still travel far and wide, may never be).

Sens. Rubio and Warner have sounded this alarm before. They have said that deepfakes and other doctored or fabricated

video should be considered a national security concern, especially related to election interference.

Unfortunately, manipulated, fake videos don’t have to rely on the latest in AI technology to be seriously misleading, as Sen. Warner pointed out in a tweet. “Whether we’re talking about deepfakes or more low-tech synthetic media like [what] slowed down video of [House] Speaker [Nancy] Pelosi, we’re facing a serious threat to public trust in the information we consume,” Warner said. “We ought to know if social media companies have a plan for how to deal with this.”

https://arstechnica.com/?p=1578591

Why Ajit Pai’s “unhinged” net neutrality repeal was upheld by judges

Enlarge / FCC Chairman Ajit Pai with his oversized coffee mug in November 2017.

reader comments

157 with 98 posters participating, including story author

Share this story

The Federal Communications Commission has mostly defeated net neutrality supporters in court even though judges expressed skepticism about Chairman Ajit Pai’s justification for

repealing net neutrality rules.

One of the three judges who decided the case wrote that the FCC's justification for reclassifying broadband "is unhinged from the realities of modern broadband service." But all three judges who ruled on the case agreed that they had to leave the net neutrality repeal in place based on US law and a Supreme Court precedent (see ruling).

The case at the US Court of Appeals for the District of Columbia Circuit turned on the FCC's decision to reclassify broadband as an information service instead of as a telecommunications service. Telecommunications services are regulated under common-carrier laws, which provided the legal basis for net neutrality rules. The act of reclassifying broadband as an information service deregulated the broadband industry and removed the legal underpinning for the net neutrality rules.

The FCC has broad authority to classify offerings as either information services or telecommunications as long as it provides a reasonable justification for its decision. Judges can disagree with the FCC's reasoning and still uphold the classification if the FCC provides a good-enough explanation.

To defend the reclassification, the FCC had to explain why broadband fits the federal definition of "information service" and not the federal definition of "telecommunications service." Under US law, telecommunications is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."

That *sounds* like what broadband companies provide, but the FCC claims that broadband isn't telecommunications because Internet providers also offer DNS (Domain Name System) services and caching as part of the broadband package. According to the FCC, the offering of DNS and caching makes

broadband an information service, which is defined under US law as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."

Judges reluctantly ruled that the FCC made a permissible reading of the statute.

Brand X ties judges' hands

The Supreme Court's 2005 decision in the *Brand X* case, which let the FCC classify cable broadband as an information service, is what basically forced judges to allow the FCC's new interpretation of broadband. In her concurring opinion, Circuit Judge Patricia Millett explained that *Brand X* "compels us to affirm as a reasonable option the agency's reclassification of broadband as an information service based on its provision of Domain Name System ('DNS') and caching. But I am deeply concerned that the result is unhinged from the realities of modern broadband service."

Millett is concerned because the nature of broadband offerings has changed dramatically since *Brand X.* She wrote:

> *Brand X was decided almost 15 years ago, during the bygone era of iPods, AOL, and Razr flip phones. The market for broadband access has changed dramatically in the interim. Brand X faced a "walled garden" reality, in which broadband was valued not merely as a means to access third-party content but also for its bundling of then-nascent information services like private email, user newsgroups, and personal webpage development. Today, none of those add-ons occupy the significance that they used to.*

Today, consumers use broadband almost exclusively to access third-party content. "In a nutshell, a speedy pathway to

content is what consumers value. It is what broadband providers advertise and compete over," Judge Millett wrote.

While auxiliary services like DNS and caching are still part of the broadband bundle, "their salience has waned significantly since *Brand X* was decided" in part because DNS is readily available for free from other sources, and "caching has been fundamentally stymied by the explosion of Internet encryption," Millett wrote.

"For these accessories [DNS and caching] to singlehandedly drive the Commission's classification decision is to confuse the leash for the dog," she wrote. In 2019, she continued, "hanging the legal status of Internet broadband services on DNS and caching blinks technological reality."

Judges defer to Supreme Court

Circuit Judge Robert Wilkins agreed with Millett's assessment. "As Judge Millett's concurring opinion persuasively explains, we are bound by the Supreme Court's decision in [*Brand X*], even though critical aspects of broadband Internet technology and marketing underpinning the Court's decision have drastically changed since 2005," he wrote. "But revisiting *Brand X* is a task for the [Supreme] Court—in its wisdom—not us."

Senior Circuit Judge Stephen Williams didn't join the other two judges in this line of criticism. But the statements from Millett and Wilkins demonstrate why even judges who are skeptical of the FCC's classification didn't vote against the agency on this key point. The majority opinion held that classifying broadband as an information service based on the functionalities of DNS and caching is "a reasonable policy choice."

The court quoted its own 2016 ruling in the case that upheld the Obama-era FCC's net neutrality order. That case and the

current one both upheld FCC classification decisions, even though the FCC decisions themselves were polar opposites.

Yesterday's court ruling said:

> *As we said in [the previous net neutrality case], "Our job is to ensure that an agency has acted 'within the limits of [Congress'] delegation' of authority," and "we do not 'inquire as to whether the agency's decision is wise as a policy matter; indeed, we are forbidden from substituting our judgment for that of the agency.'"*

Judges also accepted the FCC's explanation "for believing that competition exists in the broadband market," including the claim that customers with only one choice can benefit from competition elsewhere. The FCC claimed that a consumer in an area with fewer than two providers may benefit from competition because the provider in this area "will tend to treat customers that do not have a competitive choice as if they do." That's because competitive pressures elsewhere "often have spillover effects across a given corporation."

"Based on these reasonable findings and our highly deferential standard of review, it was not arbitrary for the Commission to conclude that fixed broadband providers face competitive pressures," judges concluded.

Decision keeps net neutrality rules off the books

Yesterday's ruling was issued in response to an appeal filed by a coalition of state attorneys general, consumer advocacy groups, and tech companies such as Mozilla and Vimeo.

Despite upholding the net neutrality repeal and broadband classification, judges remanded the decision to the FCC, forcing the commission to clear up a few points. On remand,

the FCC must explain what the repeal means for public safety, for the regulation of pole attachments, and for the Lifeline program that subsidizes phone and Internet access for low-income Americans.

But judges said that the details of the case "weigh in favor of remand without *vacatur*." This means that the repeal of net neutrality rules will remain in place even while the FCC deals with the remanded issues.

Judges wrote:

> *First, the Commission may well be able to address on remand the issues it failed to adequately consider in the 2018 Order… Second, the burdens of vacatur on both the regulated parties (or non-regulated parties as it may be) and the Commission counsel in favor of providing the Commission with an opportunity to rectify its errors. Regulation of broadband Internet has been the subject of protracted litigation, with broadband providers subjected to and then released from common-carrier regulation over the previous decade. We decline to yet again flick the on-off switch of common-carrier regulation under these circumstances.*

Why FCC can't easily preempt state laws

The only big loss for the FCC came during its attempt to prevent all 50 states from passing their own net neutrality laws. Judges vacated the FCC's attempt at a blanket, nationwide preemption, although the FCC can still try to preempt future laws on a case-by-case basis.

"At bottom, the Commission lacked the legal authority to categorically abolish all 50 States' statutorily conferred authority to regulate intrastate communications," judges wrote.

This isn’t a completely free pass for states to regulate broadband providers, but the FCC could still find it difficult to preempt specific laws. The FCC argued that state net neutrality laws would violate a federal policy of non-regulation and that broadband “is an interstate service that should be subject to uniform regulation.”

But the FCC’s opponents argued that the FCC cannot preempt state and local net neutrality laws because the commission abandoned its Title II regulatory authority over broadband. Two of the three judges agreed.

“[I]n any area where the Commission lacks the authority to regulate, it equally lacks the power to preempt state law,” the majority opinion said. The FCC’s “affirmative” sources of regulatory authority come from Title II, III, and VI of the Communications Act, judges wrote. But Pai’s FCC chose to apply Title I to broadband, which contains no such authority.

“It is Congress to which the Constitution assigns the power to set the metes and bounds of agency authority, especially when agency authority would otherwise tramp on the power of States to act,” the majority opinion said. In order for the FCC to preempt state laws using Title I, “the agency’s interpretive authority would have to trump Congress’s calibrated assignment of regulatory authority in the Communications Act,” the opinion said.

Self-made agency policy

The ruling also said that preemption “cannot be a mere byproduct of self-made agency policy” when Congress has not granted authority to preempt. The ruling added that this principle applies “Doubly so here where preemption treads into an area—State regulation of intrastate communications—over which Congress expressly ‘deni[ed]’ the Commission regulatory authority.” (Broadband transmissions consist of both interstate and intrastate communications.)

Judge Williams, who dissented on the preemption ruling, argued that the FCC can preempt state laws even in areas where it isn't using its "affirmative regulatory authority." The FCC can develop a "national telecommunications policy" without using its Title II powers over common carriers, Williams wrote.

But the majority said the FCC hasn't made a showing that wiping out all potential state and local requirements is necessary to achieve the FCC's deregulatory objectives. If the FCC wants to preempt a specific state law in the future, it will have to "explain how a state practice actually undermines the 2018 Order," judges wrote. If the FCC "cannot make that showing, then presumably the two regulations can co-exist as the Federal Communications Act envisions."

https://arstechnica.com/?p=1578617

Facebook tried to fight $5B FTC fine, is ready to fight antitrust probes

reader comments

120 with 55 posters participating

Share this story

Facebook's $5 billion settlement with the Federal Trade

Commission this summer smashed records: the FTC had never before fined any company such a hefty amount. But even though critics immediately lambasted the deal as a comparative slap on the wrist for Facebook, which earned about $56 billion in revenue in 2018, newly released documents show that the company was working hard to avoid any penalty at all—and its arguments then are just a prelude to defenses it may mount now, as dozens of state, federal, and international probes pile up around it.

Facebook made its claims to the FTC in a February 28 memo (PDF), which was independently obtained and published Monday by both The Hill and The Washington Post.

In the memo, Facebook argued that the fine is unconstitutional, saying that it violates both the due process clause as well as the excessive fines clause of the Eighth Amendment. “No court would impose such a plainly excessive and disproportionate penalty,” the company said. “The proposed penalty is wildly disproportionate to any harm suffered.”

“Facebook is prepared to prove with expert analysis that, in fact, no consumer harm occurred as a result of the alleged order violations,” the company continued, saying that it “did not profit from the alleged violations.” Instead, Facebook argued, its fine, if any, should be more in line with the $22.5 million Google paid in 2012 following allegations it installed tracking cookies on the Safari browser by circumventing default user settings.

The harms suffered

The $5 billion settlement addressed several different allegations. Primary among them: Facebook had been through this before. The company and the FTC reached a settlement in 2011 requiring Facebook privacy settings and information sharing to be “opt-in” and mandating 20 years of regular privacy audits for the company.

The 2019 settlement found those updated settings, and their outcomes, to be misleading. “At least tens of millions of American users relied on Facebook’s deceptive privacy settings and statements to restrict the sharing of their information,” the complaint said, “When, in fact, third-party developers could access and collect their data through their friends’ use of third-party developers’ apps.”

The most notorious of those third parties was Cambridge Analytica, which used the Facebook API not only to collect data from the 270,000 individuals who used its personality-quiz app but also from all those users’ friends. Facebook said in 2018 that up to 87 million users may have had their data “improperly shared” with Cambridge Analytica which, in turn, shared it with the Trump presidential campaign.

Had Cambridge Analytica been the only instance in which Facebook users’ privacy was violated in unexpected ways, perhaps the FTC would have been more lenient. But the commission also said Facebook violated the 2011 order by “misrepresenting” consumers’ ability to opt out of facial recognition, by storing user passwords without encryption, and by using phone numbers provided for two-factor authentication for advertising purposes without permission.

The privacy issues with third-party apps did not magically end with either the nominal dissolution of Cambridge Analytica or the FTC settlement. As recently as September 20, Facebook suspended tens of thousands of apps from its platform after they were found to be violating users’ privacy. The company also filed suit against developers who allegedly used quiz apps to scrape users’ data.

Facebook’s warmup routine

The entire Cambridge Analytica scandal—all the congressional hearings and testimony, the media reports, the $5 billion settlement—may pale in scope compared to the regulatory fight

that Facebook faces today. In the United States alone, Facebook is the current target of wide-reaching antitrust investigations being conducted by Congress, the FTC, the Justice Department, and several states.

Many of those probes focus on Facebook's history of acquiring former competitors such as Instagram and WhatsApp, and critics are increasingly calling for the company to be broken back up along those lines. Most notable among those voices is Sen. Elizabeth Warren (D-Mass.), who in March announced a plan for doing just that as one of the policy planks of her 2020 campaign. Facebook and its CEO Mark Zuckerberg, as you might imagine, are not thrilled about the idea.

The Verge today published leaked audio it obtained of Zuckerberg discussing the potential for future regulatory action at a pair of employee meetings held in July.

"I'm certainly more worried that someone is going to *try* to break up our company," Zuckerberg said. "There might be a political movement where people are angry at the tech companies, or are worried about concentration, or worried about different issues and worried that they're not being handled well."

"If [Warren] gets elected president, then I would bet that we will have a legal challenge, and I would bet that we will win the legal challenge," he prophesied. "And does that still suck for us? Yeah. I mean, I don't want to have a major lawsuit against our own government… But look, at the end of the day, if someone's going to try to threaten something that existential, you go to the mat, and you fight."

The fight, he argued, would be entirely justified because breaking up Facebook wouldn't help anything. "Breaking up these companies, whether it's Facebook or Google or Amazon, is not actually going to solve the issues," Zuckerberg told employees. "It doesn't make election interference less likely.

It makes it more likely because now the companies can’t coordinate and work together.”

Zuckerberg concluded his thoughts on the matter by saying:

> *So yes, I think that the direction of the discussion is concerning. I at least believe, I think, there are real issues. I don’t think that the antitrust remedies are going to solve them. But I understand that if we don’t help address those issues and help put in place a regulatory framework where people feel like there’s real accountability and the government can govern our sector, then yeah, people are just going to keep on getting angrier and angrier. And they’re going to demand more extreme measures, and, eventually, people just say, “Screw it, take a hammer to the whole thing.” And that’s when the rule of law comes in, and I’m very grateful that we have it.*

https://arstechnica.com/?p=1577309

Why big ISPs aren’t happy about Google’s plans for encrypted DNS

reader comments

142 with 77 posters participating

Share this story

When you visit a new website, your computer probably submits a request to the domain name system (DNS) to translate the domain name (like arstechnica.com) to an IP address. Currently, most DNS queries are unencrypted, which raises privacy and security concerns. Google and Mozilla are trying to address these concerns by adding support in their browsers for sending DNS queries over the encrypted HTTPS protocol.

But major Internet service providers have cried foul. In a September 19 letter to Congress, Big Cable and other telecom industry groups warned that Google's support for DNS over HTTPS (DOH) "could interfere on a mass scale with critical Internet functions, as well as raise data-competition issues."

On Sunday, the *Wall Street Journal* reported that the House Judiciary Committee is taking these concerns seriously. In a September 13 letter, the Judiciary Committee asked Google for details about its DOH plans—including whether Google plans to use data collected via the new protocol for commercial purposes.

But Google says that these concerns are groundless. Despite insinuations from telecom companies, Google says, the company has no plans to switch Chrome users to its own DNS servers. And while Google didn't mention it, the company has plenty of ways to monitor users' browsing patterns with or without access to their DNS queries.

The telecom industry letter is confusing because it mashes together two different criticisms of Google's DOH plans. One concern is that switching to encrypted DNS would prevent ISPs and others from spying on their users. The other is that, in the process of enabling DOH, Google will switch millions of users over to Google's own DNS servers, leading to a dangerous concentration of control over DNS.

Understanding the debate is easier if we consider each of these concerns separately.

Google says it isn’t planning to switch users to its DNS

Let’s start with the second concern: that Google will switch Chrome users to its own DNS servers, giving Google concentrated power over DNS. Google’s response here is simple.

“Google has no plans to centralize or change people’s DNS providers to Google by default,” the company said in an email to Ars Technica. “Any claim that we are trying to become the centralized encrypted DNS provider is inaccurate.”

Google laid out its plans in detail in a September 10 blog post. Starting with version 78, Chrome will begin experimenting with the new DOH feature. Under the experiment, Chrome will “check if the user’s current DNS provider is among a list of DoH-compatible providers, and upgrade to the equivalent DoH service from the same provider,” Google wrote. “If the DNS provider isn’t in the list, Chrome will continue to operate as it does today.”

One possible reason for confusion on this point is that Mozilla is planning a more aggressive rollout of the technology. The company is planning to gradually shift all of its users to DOH—whether or not their existing DNS provider supports it. The shift will make Cloudflare the default DNS provider for many Firefox users, regardless of the DNS settings of the underlying OS.

Mozilla has more latitude to do this because most surveys show Firefox with single-digit market share—and Firefox isn’t a major DNS provider in its own right. So there’d be little basis for antitrust scrutiny if Mozilla shifts its users over to a new DNS provider. The same move could raise antitrust

concerns if Google started switching Chrome users over to its own DNS. But Google says it has no plans to do that.

DNS over HTTPS means ISPs can’t spy on their users

Enlarge / Google CEO Sundar Pichai.
Simon Dawson/Bloomberg via Getty Images

Telecom companies also raised a second concern that applies even if Google doesn’t shift anyone to its own DNS servers. Put simply: the lack of DNS encryption is convenient for ISPs.

ISPs sometimes find it useful to monitor their customers’ Internet traffic. For example, queries to malware-associated domains can be a signal that a customer’s computer is infected with malware. In some cases, ISPs also modify customers DNS queries in-flight. For example, an easy way to block children from accessing adult materials is with an ISP-level filter that re-writes DNS queries for banned domains. Some public Wi-Fi networks use modified DNS queries as a way to redirect

users to a network sign-on page.

Some ISPs also use DNS snooping for more controversial purposes—like ad targeting or policing their networks for copyright infringement.

Widespread adoption of DOH would limit ISPs' ability to both monitor and modify customer queries. It wouldn't necessarily eliminate this ability, since ISPs could still use these techniques for customers who use the ISP's own DNS servers. But if customers switched to third-party DNS servers—either from Google or one of its various competitors—then ISPs would no longer have an easy way to tell which sites customers were accessing.

ISPs could still see which IP addresses a customer had accessed, which would give them some information—this can be an effective way to detect malware infections, for example. But this is a cruder way to monitor Internet traffic. Multiple domains can share a single IP address, and domains can change IP addresses over time. So ISPs would wind up with reduced visibility into their customers' browsing habits.

What would a switch mean?

But a switch to DOH would clearly mean ISPs had less ability to monitor and manipulate their customers' browsing activity. Indeed, for advocates that's the point. They believe users, not their ISPs, should be in charge.

Mozilla, which is pushing DOH more aggressively than Google, has taken steps to avoid creating too much chaos in the process. In July, Mozilla said that it wouldn't enable DOH by default in the UK, where ISPs are planning to use DNS to implement legally mandated porn filtering.

Before enabling DOH, Firefox will check if a computer has parental control software installed. In enterprise settings,

Mozilla will try to figure out if a switch to DOH will break corporate Intranet features that depend on using specific DNS servers. Firefox will continue using the existing DNS servers in these cases.

So far, Google is only enabling DOH for a selected number of whitelisted DNS providers, so the switch shouldn't cause too many problems. If the company goes beyond that, we can expect it to take measures similar to those Mozilla has taken.

In any event, it's hard to see a policy problem here. ISPs' ability to eavesdrop on their customers' DNS queries is little more than an historical accident. In recent years, websites across the Internet have adopted SSL encryption for the contents of their sites. The encryption of DNS is the natural next step toward a more secure Internet. It may require some painful adjustments by ISPs, but that hardly seems like a reason for policymakers to block the change.

https://arstechnica.com/?p=1576941

Councilman "mind-boggled" by Baltimore City IT department ineptitude

Enlarge / This is Baltimore, gentlemen. The gods will not save you…from ransomware.

reader comments

87 with 77 posters participating, including story author

Share this story

In a report to a committee of the Baltimore City Council last week, City Auditor Josh Pasch said that the city's Information Technology department could not provide any documentation of its work toward meeting agency performance goals because the only copies of that data were kept on local hard drives and never backed up to a server or the cloud.

As the Baltimore Sun's Luke Broadwater reports, Pasch told the council:

> *Performance measures data were saved electronically in responsible personnel's hard drives. One of the responsible personnel's hard drive was confiscated, and the other responsible personnel's selected files were removed due to the May 2019 ransomware incident…One of the things I've learned in my short time here is a great number of Baltimore City employees store entity information on their local computers. And that's it.*

The lost data, Pasch said, resulted in a "loss of confidence" in whether the IT department was accomplishing anything on its to-do list.

City Councilman Eric T. Costello interrupted the testimony to interject, "That can't be right? That's real?… Wow. That's mind-boggling to me."

In a written statement to the committee, Baltimore City Chief Information Officer Frank Johnson acknowledged the findings of the audit and said that his agency would work to improve the department's data-storage practices. Johnson, however, is on "extended leave" from the agency. It is widely believed he

will not return, according to sources in Baltimore City government who spoke to Ars Technica. Johnson, who was hired by the now-resigned Mayor Catherine Pugh, was previously a regional vice president of sales for Intel with no IT operations experience.

The “RobbinHood” ransomware attack against Baltimore City has thus far cost the city over $18 million. The process is made much more expensive by the widespread absence of data backups or any sort of disaster recovery planning. Over the summer, temporary workers were brought in to replace hard drives and monitors on affected computers, and new servers were purchased to replace those affected by the ransomware.

Ars has requested information from the city regarding the contracting details for the recovery, but the city has thus far provided no data. Requests for data on the status of patches and disaster recovery plans were refused because the documents do not exist as a result of the ransomware attack.

https://arstechnica.com/?p=1577269

NCAA fights California over new law that helps athletes get paid

Enlarge / Mississippi Rebels and Xavier Musketeers go head-to-head during the second round of the 2015 NCAA Men’s Basketball on March 19, 2015, in Jacksonville, Florida.

reader comments

105 with 65 posters participating

Share this story

California Governor Gavin Newsom today signed a bill into law allowing college athletes to get paid for endorsements, setting up a battle between the state government and the NCAA.

The NCAA strongly opposes California's Fair Play to Pay Act and has threatened to sue the state and prohibit California colleges from competing in NCAA events, even though the new law doesn't actually require colleges to pay athletes. Instead, the act allows student athletes to hire agents and get paid by third parties for sports-related endorsements.

"Colleges and universities reap billions from these student athletes' sacrifices and success but block them from earning a single dollar. That's a bankrupt model," Newsom said in his announcement of the bill signing. When it takes effect in 2023, the new law will make California "the first state in the nation to allow student athletes to receive compensation from the use of their name, image, and likeness," the announcement said.

Here's how the bill achieves that goal, as explained in Newsom's press release:

> *Starting on January 1, 2023, the Fair Pay to Play Act will allow all student athletes enrolled in public and private four-year colleges and universities in California to earn money from their name, image, or likeness. Student athletes will also be able to hire sports agents and not lose their scholarships if they receive income for their work. Further, SB 206 prohibits California colleges from enforcing NCAA rules that prevent student athletes from earning compensation and will prevent the NCAA from banning California universities from intercollegiate sports if their athletes*

sign sponsorship deals.

NCAA continues opposition

The bill was inspired partly by former UCLA basketball star Ed O'Bannon's lawsuit against the NCAA over the use of athletes' images in video games and other types of media. O'Bannon became the lead plaintiff in the antitrust class action after his likeness was used in the Electronic Arts game *NCAA Basketball 09*. O'Bannon's side achieved a partial victory in the case against the NCAA, and players obtained a $60 million settlement from Electronic Arts, which reportedly amounted to an average of $1,600 per player.

The case ultimately didn't have much impact on actual NCAA policies, and it helped prevent production of more college sports games. "The lawsuit filed against Electronic Arts and the NCAA resulted in the discontinuation of the college video game franchise," ESPN wrote at the time of the settlement. "*NCAA Football 14*, which hit shelves in July 2013, was the last game that was produced." The similar NCAA basketball series of video games was discontinued after the 2010 edition.

Theoretically, the California law could pave the way for officially licensed NCAA sports video games that benefit schools *and* players financially. But that isn't likely to happen as long as the NCAA continues to oppose payments to athletes in any form.

The NCAA urged Gov. Newsom to reject the bill in a letter that threatened to bar California universities from NCAA competitions. The NCAA said the California bill "would erase the critical distinction between college and professional athletics and, because it gives those schools an unfair recruiting advantage, would result in them eventually being unable to compete in NCAA competitions."

Of course, the NCAA could eliminate what it called California's "unfair recruiting advantage" by changing its rules to let student athletes in all states earn endorsements. The NCAA's amateurism rules say that student athletes may not "promote or endorse a product or allow their name, image, or likeness to be used for commercial or promotional purposes." Violating the rule would prevent athletes from getting the "amateurism certification" they need to compete in NCAA sports.

The NCAA letter called the California bill "unconstitutional," suggesting that the organization might sue the state to prevent its implementation. The NCAA also said it's working to change its rules but did not commit to actually letting athletes get any money.

"NCAA member schools already are working on changing rules for all student athletes to appropriately use their name, image, and likeness in accordance with our values—but not pay them to play," the NCAA said.

The NCAA issued another statement today after Newsom signed the bill. The NCAA said that it "will consider next steps in California while our members move forward with ongoing efforts to make adjustments to NCAA name, image, and likeness rules that are both realistic in modern society and tied to higher education." The new NCAA statement also claimed that the new law is "creating confusion for current and future student athletes, coaches, administrators, and campuses."

Thumbs up from athletes

Newsom signed the bill on an episode of HBO's *The Shop: Uninterrupted*, appearing alongside LeBron James, O'Bannon, UCLA gymnast Katelyn Ohashi, and WNBA player Diana Taurasi.

"Athletes at every level deserve to be empowered and to be fairly compensated for their work, especially in a system

where so many are profiting off of their talents," James said.

The bill was sponsored in the California Senate by Sens. Nancy Skinner (D-Berkeley) and Senator Steven Bradford (D-Gardena). Skinner said the bill "makes California the first state to restore to student athletes a right everyone else has: the right to earn money from their name, image, and likeness."

Bradford said the new law addresses an important civil rights issue and that "colleges and universities should no longer treat student athletes as chattel."

"While our student athletes struggle to get by with basic necessities such as food and clothing, universities and the NCAA make millions off of their talent and labor," Bradford said. "College coaches are now some of the highest paid employees in the country because of the talented young men and women who play for them."

Newsom suggested that other states will replicate California's new law. "This is the beginning of a national movement—one that transcends geographic and partisan lines," Newsom said.

https://arstechnica.com/?p=1577131

Feds say Boeing 737 needs to be better designed for humans

reader comments

149 with 68 posters participating

Share this story

The two 737 MAX crashes that killed 346 people and led to what is, so far, a six-month grounding of the jet, stemmed in part from Boeing's failure to accurately anticipate how pilots would respond to a malfunctioning feature that pointed the jets toward the ground. That's the key finding from a report the National Transportation Safety Board published Thursday, which included a series of recommendations to the Federal Aviation Administration. The NTSB advised the regulator to have Boeing consider how 737 MAX pilots would handle not just problems with the MCAS system alone, but how they respond to multiple simultaneous alerts and indicators. In short, the NTSB says Boeing was wrong to assume pilots would respond correctly to the problem that ended up killing them.

The crashes of Lion Air Flight 610, in October 2018, and Ethiopian Airlines Flight 302, in March, stemmed from a feature Boeing designed to prevent stalls. In both cases, the Maneuvering Characteristics Augmentation System, or MCAS, activated in response to a false reading from a faulty angle of attack sensor. The pilots fought to counteract the system, which pushed the nose of the plane down, but ultimately failed.

When Boeing tested what would happen if the MCAS malfunctioned, it didn't account for other elements. The Lion Air and Ethiopian pilots on the doomed planes dealt with a cascade of problems and warnings: Their control sticks shook. Various alarms sounded. When the pilots retracted the flaps, the plane's downward push required extra force to keep the jet aloft. The result: Their reactions "did not match [Boeing's] assumptions," the NTSB found. "An aircraft system should be designed such that the consequences of any human error are limited."

The FAA hasn’t said whether it will adopt the recommendations of the NTSB, which has no regulatory or enforcement power. And this is far from the end of the 737 MAX saga: Boeing and the FAA are still negotiating a fix to the plane’s software, and congressional, international, and criminal investigations into the crashes are ongoing.

But as its title—“Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance”—indicates, the NTSB report is about more than one troubled jet, one feature, one company, or even one country. The safety board wants the FAA to apply this sort of thinking to all the planes it certifies. And it hopes the agency will encourage its peers around the world to do the same. That’s because the report is all about the question at the core of modern aviation safety: How to ensure that pilots can work with the computers that have taken on more of the work in the cockpit. It’s about a field of study called “human factors.”

“The field of aviation has been the cradle of human factors, and its biggest beneficiary,” says Najmedin Meshkati, who studies the field at the University of Southern California. Where ergonomics and biomechanics center on physical responses, human factors tends to center on the gray stuff packed into their skulls. It matters in fields from self-driving cars to coal mines—anywhere people interact with machines. It’s long been a major focus in aviation because so many crashes trace back to pilots’ failure to understand what the plane’s myriad and complex systems are doing, why, or how to influence them. “Whenever you have a human error, and the consequence isn’t immediately noticeable or reversible, human factors is important,” Meshkati says.

That’s often the case in aviation—and the error doesn’t always come from the human. The rising use of automation in aviation has produced major safety and practical benefits, but also distanced humans from the workings of the planes they’re

commanding. Meshkati draws a distinction between decision making and problem solving. The former is usually routine and procedure-based, like using your altitude, airspeed, and heading to calculate a landing path. Computers are very good at this. Problem solving comes in when some combination of factors means the procedures don’t work, when a person needs to absorb information and devise a new formula that will keep them safe. This is where humanity has the edge, but hardly a guaranteed victory.

According to the NTSB report, Boeing counted on pilots following a procedure that would get them out of a situation where MCAS malfunctioned. But Lion Air 610 and Ethiopian 302 demanded problem solving: Each set of pilots was fighting a plane that wanted to dive, while considering a cascade of malfunctions and signals. Better human factor thinking, Meshkati says, would have required less, or easier, problem solving. It could have produced a procedure that fit the actual conditions of the flights, allowing for good old decision making.

Of course, the FAA has other things to consider. The NTSB’s recommendations are “absolutely valid,” says Clint Balog, a flight test pilot and human factors expert with the College of Aeronautics at Embry-Riddle University. But, he says, the safety agency trends toward idealism. “The FAA has to consider, what is realistic testing?” If airplane makers had to test for every possible combination of malfunctions and cockpit alarms, they’d never get another plane certified, he says. Not all pilots are equally skilled, by virtue of their natural talent, training, or experience. It doesn’t make sense, Balog says, to design for the worst of the bunch—or the best. Cockpits as physical spaces, he points out, are designed for pilots of many shapes and sizes. But designers had to settle on limits on who can sit comfortably or reach every control. “We’ve got to figure out how to do the same thing for cognitive capability,” Balog says.

This story first appeared on wired.com.

https://arstechnica.com/?p=1575961

Nonprofit fights TV networks in court to keep free TV service alive

Getty Images | Jacobo Zanella

reader comments

79 with 51 posters participating

Share this story

A nonprofit organization that provides free online access to broadcast TV stations has accused TV networks of colluding to limit access to those channels.

The nonprofit that runs Locast, the free TV service, made the allegations in an answer to a lawsuit filed by ABC, CBS, Fox, and NBC. The networks alleged in July that Locast is violating their copyrights and are seeking a permanent injunction to shut the TV service down. The Locast operator filed its answer to the TV networks' complaint yesterday and tried to turn the tables by making several counterclaims against the TV networks.

"Plaintiffs have colluded to limit the reasonable public

access to the over-the-air signals that they are statutorily required to make available for free," Locast's court filing says. "[The networks] have opted instead to use their copyrights improperly to construct and protect a pay-TV model that forces consumers to forgo over-the-air programming or to pay cable, satellite, and online providers for access to programming that was intended to be free."

Locast cites nonprofit exemption

While broadcast TV networks are available for free over the air with an antenna, the networks reportedly collected $10.1 billion in 2018 via retransmission fees they charge TV providers for the right to carry those channels. The networks want to shut Locast down because free, widespread availability of their channels over the Internet would threaten their retransmission business.

The TV networks' lawsuit was filed in US District Court for the Southern District of New York against Sports Fans Coalition New York (SFCNY), the nonprofit that operates Locast, and SFCNY founder David Goodfriend.

Locast, available in 13 US markets so far, retransmits local broadcast signals via an online streaming service and detects users' locations so that each channel's stream is available only in the local broadcast area. SFCNY argued in its court filing that US copyright law "unambiguously states that retransmissions by non-profit entities do not constitute copyright infringement." Specifically, the law says that secondary transmissions are not copyright infringements if they are made by a "nonprofit organization, without any purpose of direct or indirect commercial advantage."

Locast doesn't charge users for its service but solicits donations to pay for its operation.

Locast: TV networks limit reach of channels

The TV networks have deliberately made it difficult to access their channels over the air despite the US government granting them "free licenses to portions of the limited, publicly owned broadcast spectrum," SFCNY alleged.

"The broadcasters have colluded to limit practical access to the over-the-air signals by broadcasting signals that they know are of insufficient strength to be accessed by all members of the public within the relevant local geographic areas," SFCNY wrote. The networks thus are not fulfilling their spectrum-license requirement "to operate in the public interest," SFCNY wrote.

The SFCNY/Locast filing continued:

> *This failure has led to poor quality over-the-air transmissions in many markets, forcing consumers to pay for video services that include local or national television programming, including: (i) through cable or satellite providers; (ii) online through the cable or satellite providers' authenticated video services; (iii) over-the-top streaming services offered by the broadcasters for a monthly fee (e.g., CBS All Access); or (iv) virtual pay-TV providers (e.g., YouTubeTV).*

SFCNY claims that broadcasters "intentionally purchase low-end equipment even though other equipment is available for sale that could provide better over-the-air coverage," but doesn't seem to have direct evidence for this claim. The filing says that Goodfriend got this information "from a major market participant" who had in turn been given the information "by vendors of transmitter equipment."

SFCNY also wrote that networks have prohibited their local

broadcast affiliates from providing online streaming of over-the-air live television broadcasts, the court filing said.

No Locast on YouTube TV

TV networks have also pressured TV providers to avoid partnering with Locast, according to Locast's filing. For example, when Locast met with senior executives at YouTube TV in April 2019, "the executives indicated that they had been told that if YouTube TV provides access to Locast, then YouTube TV will be punished by the Big 4 broadcasters in negotiating carriage agreements for other non-broadcast programming channels," SFCNY's court filing said.

Pay-TV providers have complained about the high cost of retransmitting broadcast TV channels and could benefit from an expansion of Locast service. Locast received a $500,000 donation from AT&T but says the TV networks pressured others to refrain from donating.

In addition to filing "a sham copyright infringement claim" against Locast, networks have been "threatening business retaliation and baseless legal claims against any current or prospective donors, supporters, or business partners of Counterclaim-Plaintiffs," Locast claimed. Cable company RCN "committed to donating $750,000 to SFCNY" but later decided not to because of "intimidation from the broadcasters," SFCNY claimed.

The TV networks argue that Locast isn't eligible for the nonprofit exemption under copyright law because it has "commercial purposes." The networks' evidence for this is AT&T's $500,000 donation and the fact that Goodfriend is a paid lobbyist for Dish. SFCNY says it hasn't received any funding from Dish.

SFCNY accuses the TV networks of conspiracy in restraint of trade and other violations of competition laws and seeks

financial damages and an injunction that would prevent the networks from continuing their copyright infringement lawsuit. “Plaintiffs’ litigation is meant to intimidate Defendants into shuttering the Locast service—and should that strategy not work, to bury Defendants under costly and needless litigation,” SFCNY wrote.

The law firm representing broadcast networks in the case contacted Ars with the following statement responding to the Locast filing:

> *Locast’s filing only confirms that it has no answer for its industrial scale violations of the law. Sixteen million households receive broadcast television free over the air, which represents a nearly 50 percent increase in the last eight years. Locast does nothing for those households; it serves the interests of its pay-TV patrons, who have provided Locast and its founder with hundreds of thousands of dollars in lobbying fees, donations and nationwide distribution on certain pay-TV platforms. We trust the courts to see right through this façade and recognize Locast for what it is—not a public service organization, but a creature of certain pay-TV interests with an entirely commercial agenda.*

https://arstechnica.com/?p=1576083