Tesla threatened to sue buyers who resell Cybertruck without written permission

Enlarge / The Tesla Cybertruck.

reader comments

237 with

With Tesla's first Cybertruck deliveries expected later this month, a now-deleted update to the electric carmaker's terms of service said the firm could sue customers for $50,000 or more if they resell during the first year of ownership without first getting written permission from Tesla. The provision seemed designed to deter scalping for a car expected to be available only in limited quantities after CEO Elon Musk's statement that Tesla "dug our own grave with the Cybertruck."

But the clause was deleted from Tesla's terms just days after people noticed its appearance. It was still in the Tesla Motor Vehicle Order Agreement Terms & Conditions earlier today, but was removed from the document while we worked on this article. The document still has a more general rule against quick resales but without the lawsuit threat.

Tesla may have decided to remove the clause after several news reports spread word of the change over the weekend. It's not clear whether the company will bring the clause back in a modified form. We contacted Tesla and will update this article if we get a response.

Before the deletion, the document said Cybertruck buyers had

to offer the car back to Tesla before any attempt to resell the vehicle within one year of delivery. If Tesla declines to buy the Cybertruck back, the owner could resell it only if Tesla provides "written consent." Tesla said it would seek an injunction and financial damages if you violate the provision, or if "Tesla has reasonable belief that you are about to breach this provision."

Advertisement

"Tesla may seek injunctive relief"

The now-deleted clause read as follows:

> *You understand and acknowledge that the Cybertruck will first be released in limited quantity. You agree that you will not sell or otherwise attempt to sell the Vehicle within the first year following your Vehicle's delivery date. Notwithstanding the foregoing, if you must sell the Vehicle within the first year following its delivery date for any unforeseen reason, and Tesla agrees that your reason warrants an exception to its no reseller policy, you agree to notify Tesla in writing and give Tesla reasonable time to purchase the Vehicle from you at its sole discretion and at the purchase price listed on your Final Price Sheet less $0.25/mile driven, reasonable wear and tear, and the cost to repair the Vehicle to Tesla's Used Vehicle Cosmetic and Mechanical Standards.*
>
> *If Tesla declines to purchase your Vehicle, you may then resell your Vehicle to a third party only after receiving written consent from Tesla. You agree that in the event you breach this provision, or Tesla has reasonable belief that you are about to breach this provision, Tesla may seek injunctive relief to prevent the transfer of title of the Vehicle or demand liquidated damages from you in the amount of $50,000 or the value received as consideration for the sale or transfer, whichever is greater. Tesla may also refuse*

to sell you any future vehicles.

Here’s a screenshot of the clause that we took earlier today:

The Cybertruck was first revealed in 2019. According to Car and Driver, it is expected to cost about $70,000 for a dual-motor version and $80,000 for a three-motor version. “While a starting price of about $40,000 was touted at the Cybertruck’s reveal back in 2019, that price was attached to a single-motor rear-wheel drive model,” Can and Driver wrote. “For the Cybertruck’s first year on the market though, governmental documents indicate that Tesla will only offer dual- and tri-motor all-wheel drive models which will carry higher starting prices.”

https://arstechnica.com/?p=1983454

Zelle finally caves after years of refusing to refund scam victims

reader comments

71 with

After scammers spent years swiping hundreds of millions from Zelle users by inducing people to authorize fraudulent payments, lawmakers were horrified to discover in fall 2022 that “the vast majority” of defrauded Zelle users never got their money back. To regulators, it seemed like Zelle was shirking responsibility for policing this increasingly common fraudulent activity on its payments platform.

But now, Zelle has changed its mind and is working harder to protect users from imposter scams. On Monday, Zelle confirmed that at the end of June, the payments app finally started refunding users targeted by scammers.

According to Reuters, this was possible because Zelle’s network operator, Early Warning Services (EWS), found a solution that lets Zelle’s network of 2,100 financial firms off the hook for reimbursing transactions where “potentially billions of dollars” might be stolen by imposter scammers. Instead of expecting financial partners to foot the bill to cover this fraudulent activity, Zelle simply “implemented a mechanism that allows banks to claw back funds from the recipient’s account and return them to the sender.”

“As the operator of Zelle, we continuously review and update our operating rules and technology practices to improve the consumer experience and address the dynamic nature of fraud and scams,” an EWS spokesperson told Ars. “As of June 30, 2023, our bank and credit union participants must reimburse consumers for qualifying imposter scams, like when a scammer impersonates a bank to trick a consumer into sending them money with Zelle. The change ensures consistency across our network and goes beyond legal requirements.”

Advertisement

This is the first time EWS has provided details on its new policy to refund victims of the Zelle imposter scam, Reuters reported. It's a major policy reversal that Reuters said was likely prompted to spare banks and payments apps from stricter regulatory interventions that would require refunds for every scam victim. (Currently, the US only requires banks to refund any fraudulent payments made without customers' authorization.)

The chief fraud risk officer at EWS, Ben Chance, reiterated to Reuters that Zelle's new policy goes "well above existing legal and regulatory requirements."

It's unclear if regulators will be satisfied leaving this matter to banks and payment apps, though. There may be just too many people using payment apps to ignore gaps in laws intended to protect against financial fraud. Between 2018 and 2022, peer-to-peer (P2P) payments quadrupled in the US, the Consumer Financial Protection Bureau (CFPB) reported, and by 2027, P2P payments "may reach nearly $1.6 trillion."

Meanwhile, as P2P payments have increased substantially, these imposter scams have become "the most-reported scam," targeting users "across all payment methods," the Federal Trade Commission (FTC) reported. In total, the FTC said that scam victims lost $2.6 billion last year alone.

The CFPB previously mulled new laws that would require lenders to reimburse scam victims, but a person familiar with the matter told Reuters that the CFPB may no longer be considering new protections, because Zelle's recent changes "have so far satisfied the agency." However, Senator Elizabeth Warren (D-Mass.)—who spearheaded the probe into Zelle imposter scams—told Reuters that she is not likely to stop monitoring the situation any time soon.

"Zelle's platform changes are long overdue," Warren said. "The CFPB is standing with consumers, and I urge the agency to keep

the pressure on Zelle to protect consumers from bad actors.”

https://arstechnica.com/?p=1983390

Alexa just cost Amazon another $46.7 million

Enlarge / The first Amazon Echo speaker.
Luke MacGregor/Bloomberg via Getty Images

reader comments

25 with

A Delaware federal court has ordered Amazon to pay $46.7 million for infringing on four patents belonging to VB Assets with Amazon’s Echo smart speakers and Alexa virtual assistant. A lawsuit from Nuance Communications-owned VB Assets, previously known as VoiceBox Technologies, claimed to have already invented a circular speaker that could connect to the web and answer voice-dictated prompts with a female, robotic voice.

Wednesday’s judgment [PDF], initially reported by Reuters, orders Amazon to pay the sum via running royalty rather than a lump sum. The ruling follows a jury verdict [PDF] finding that Amazon infringed upon four of VoiceBox’s patents. The patents relate to providing network-coordinated conversational services, a conversational voice user interface, and tying advertisements to natural language processing of voice-based input. VB Assets originally accused Amazon of infringing on

six of its patents.

Amazon still has time to appeal the judgment, and VoiceBox has time to seek reimbursement for related costs.

Patent infringement claims

VoiceBox claimed that it developed a prototype of something similar to Echo and Alexa long before Amazon's products were announced. In fact, its lawsuit, filed in 2019 [PDFs], included a link to a video on YouTube appearing to be a news report about VoiceBox's "Cybermind" prototype. The video seemingly shows a report from Seattle's King 5 News from 2006, demoing someone asking a speaker questions like, "Computer, what is the NBA schedule?" and "Computer, what is the forecast for Sunday?" as well as prompts, such as "Computer, find me a good recipe for chocolate cheesecake." A voice from the speaker responds to the questions or prompts, reportedly by pulling answers from the Internet or the connected computer.

You can check out the cited video and the prototype in action below:

[embedded content]
Seattle's King 5 News in 2006.
The lawsuit claimed VoiceBox's founders began work on bringing natural language understanding to computer applications in 2001. Headquartered in Bellevue, Washington, VoiceBox has made voice-controlled apps for TomTom and other GPS brands and cars, Reuters noted.

Advertisement
VoiceBox's lawsuit claimed VoiceBox demoed a voice assistant for Lexus cars called Alexus "that showcased the power of its conversational Voice technology." The lawsuit claimed that the "'Alexus' concept was introduced to the public more than six months before Amazon announced 'Alexa.'"

Like other patent cases against tech giants, the lawsuit also

claimed that Amazon invited VoiceBox employees into meetings about VoiceBox's technologies, only to end up ripping off the company's ideas and poaching employees. VoiceBox's lawsuit claimed VoiceBox first met with Amazon in 2011 "to explore a potential business relationship where VoiceBox Technologies would provide core [natural language understanding] services to Amazon." Amazon announced the Amazon Echo and Alexa in 2014. VoiceBox also claimed to have had meetings about its patents with Amazon in 2017.

Amazon didn't respond to Ars Technica's request for comment.

Another road bump for Alexa

The judgment handed down this week contrasts a 2021 ruling in a Delaware federal court finding that Alexa does not infringe upon patents by IPA Technologies Inc., as Reuters reported. While not nearly as sizeable a judgment as we've seen in other recent patent cases and a drop in the bucket in terms of Amazon's overall revenue, the ruling against Amazon comes at an inconvenient time of uncertainty and flux for its voice assistant.

At the end of 2022, Business Insider reported that Alexa was poised to lose Amazon $10 billion that year. Amazon never confirmed that figure, but there's no denying that voice assistant peddlers have been desperately brainstorming ways to try to increase the amount of revenue such technologies generate. Amazon's long-time devices head, David Limp, is also leaving the company this year.

Hoping to turn things around, Amazon in September revealed its generative AI Alexa ambitions and hopes that the voice assistant will eventually become so advanced and helpful that customers will be willing to pay a subscription fee to use its most impressive features. However, Amazon is years away from making that idea viable.

https://arstechnica.com/?p=1983039

Apple discriminated against US citizens in hiring, DOJ says

Enlarge / Apple Store at Garden State Plaza mall on November 4, 2023, in Paramus, New Jersey.
Getty Images | Gary Hershorn

reader comments

110 with

Apple illegally discriminated against US citizens and other US residents in its hiring and recruitment practices for certain types of positions that went to foreign workers, the US Department of Justice said yesterday. Apple agreed to pay up to $25 million in back pay and civil penalties to settle the DOJ allegations.

Apple discriminated "against US citizens and certain non-US citizens whose permission to live in and work in the United States does not expire," the agency said. The $25 million payment was called the largest ever collected by the Justice Department under the anti-discrimination provision of the Immigration and Nationality Act (INA).

Apple is required to pay $6.75 million in civil penalties and create an $18.25 million fund to provide back pay to those

harmed by its hiring practices. Apple did not admit guilt in the settlement. But the company acknowledged in a statement that it had “unintentionally not been following the DOJ standard,” according to Reuters.

“We have implemented a robust remediation plan to comply with the requirements of various government agencies as we continue to hire American workers and grow in the US,” Apple said. We contacted Apple and will update this article if it provides any further statement.

As Reuters noted, “Foreign labor can often be cheaper than hiring US workers, and immigrants who rely on their employers for green card sponsorship are seen as less likely to leave for a different job.”

Advertisement

DOJ investigation

The DOJ said it began investigating in February 2019 and determined “that Apple violated the INA’s anti-discrimination requirements during Apple’s recruitment for positions falling under the permanent labor certification program (PERM).” The agency said the discrimination began no later than January 1, 2018, and continued until at least December 31, 2019.

Under this program, a “permanent labor certification issued by the Department of Labor (DOL) allows an employer to hire a foreign worker to work permanently in the United States,” the DOL says. But the employer must also obtain a certification “that there are not sufficient US workers able, willing, qualified and available to accept the job opportunity in the area of intended employment and that employment of the foreign worker will not adversely affect the wages and working conditions of similarly employed US workers.”

The DOJ said its investigation “found that Apple engaged in a

pattern or practice of citizenship status discrimination in recruitment for positions it hired through PERM, and that the company's unlawful discrimination prejudiced US citizens, US nationals, lawful permanent residents, and those granted asylum or refugee status. These less effective recruitment practices deterred protected workers from applying to positions that Apple preferred to fill instead with PERM beneficiaries."

Apple did not advertise PERM positions on its external job website like it does with other positions, the DOJ said. "It also required all PERM position applicants to mail paper applications, even though the company permitted electronic applications for other positions," the DOJ said.

In some cases, "Apple did not consider certain applications for PERM positions from Apple employees if those applications were submitted electronically, as opposed to paper applications submitted through the mail," the agency said. "These less effective recruitment procedures nearly always resulted in few or no applications to PERM positions from applicants whose permission to work does not expire."

Apple changes hiring practices

The settlement requires Apple to make its PERM recruitment practices match its standard recruitment practices more closely. Apple will have to "conduct more expansive recruitment for all PERM positions, including posting PERM positions on its external job website, accepting electronic applications, and enabling applicants to PERM positions to be searchable in its applicant tracking system."

Apple has already implemented some of the changes and agreed to "train its employees on the INA's anti-discrimination requirements and be subject to departmental monitoring for the three-year period of the agreement," the DOJ said.

https://arstechnica.com/?p=1983046

Starlink bug frustrates users: “They don’t have tech support? Just a FAQ? WTF?”

Getty Images | SOPA Images

reader comments

172 with

Starlink’s lack of traditional customer support options is making life difficult today for new users affected by a bug that reset their accounts. A bunch of customers received an email from no-reply@starlink.com last night that said, “Your Starlink Account Has Been Reset. All pending orders and deposits have been refunded. You are welcome to visit Starlink.com to place a new order at any time using the same email address.”

One Ars reader who got the account-reset email contacted us about the problem, and many others are complaining in Reddit threads. Starlink’s account-recovery page that allows users to request password resets with an email address or phone number hasn’t been working for them.

“When I try to reset my password via the email option, I get the error ‘User not found,'” we were told by Adam, a Starlink customer in Alabama who preferred that we not publish his last

name. When Adam tried to reset his password by entering his phone number, he received a text message with a password-reset link. But that didn’t work, either. “After I type in a new password, I get the error message ‘User disabled,'” Adam told us.

Despite the statement about refunds, Adam didn’t have any orders or deposits refunded. He activated Starlink service on November 2 but doesn’t know if service was interrupted. “I have it at another residence, and I haven’t been there since receiving the message,” he said.

Advertisement

Starlink is operated by Elon Musk’s SpaceX corporation. We contacted SpaceX about the problem today and will update this article if we get any new information.

Enlarge / Starlink account-reset email sent by mistake to numerous customers.

“They don’t have tech support? Just

a FAQ? WTF?”

From what we’ve seen in Reddit threads, the bug doesn’t appear to disable Internet service. “I installed our Starlink two days ago, and received the email this afternoon that my account had been reset and that a refund was on the way. The Internet is still working at the moment but [I] can’t log in and submit a ticket,” one person wrote.

Another person who got the email noted that they cannot create a support ticket without being able to log in. A person in the same thread wrote, “Can’t log in and if I do a password reset request it says my account doesn’t exist. Only been using Starlink for a week. It also appears they don’t have tech support? Just a FAQ? WTF?”

Some people had Starlink dish shipments in transit when the account-reset email arrived and were concerned about whether they would be able to activate service. “Still shows my Starlink kit in transit so will create a new account with the unit if possible,” one person wrote.

“My wife got the account reset email within the last couple of hours. Tried to recover, the site says our account is disabled. Hoping there’s a resolution to this because we bought this for our new house that we’re supposed to move into next week. We haven’t even taken the dish out of the box yet,” one user wrote yesterday.

https://arstechnica.com/?p=1982976

Five big carmakers beat lawsuits alleging infotainment systems invade privacy

Enlarge / Infotainment system in a 2016 Ford Escape.
Getty Images | Todd Korol

reader comments

48 with

A federal appeals court rejected lawsuits that alleged five major carmakers violated a Washington state privacy law. The lawsuits centered on car infotainment systems that store text messages in a way that potentially allows the messages to be retrieved by law enforcement using specialized hardware and software. The rulings in the carmakers' favor came in cases against Ford, General Motors, Honda, Toyota, and Volkswagen.

A three-judge panel at the US Court of Appeals for the 9th Circuit unanimously upheld US District Court rulings that dismissed the five class-action lawsuits, which were almost identical. The appeals court ruled in Ford's favor on October 27, then issued rulings upholding the dismissals of the other four cases on Tuesday this week.

We'll cover the Ford ruling here since the other decisions don't go into the same level of detail, and the arguments were similar in all five cases. The simple version is that the cases failed because the plaintiffs' data stayed in the car systems and apparently was never transmitted to law

enforcement, Ford, or anyone else.

The class-action “complaint alleges that the vehicle’s system downloads all text messages and call logs from Plaintiffs’ cellphones as soon as they are connected,” the Ford ruling said. “The complaint also alleges that the infotainment system permanently stores the private communications without Plaintiffs’ knowledge or consent.” The complaint’s allegations refer to Ford cars made in 2014 and after.

Advertisement
Plaintiffs alleged that there is no way to delete the text messages and call logs from the car system. “If text messages or call logs are deleted from a cellphone, the vehicle nevertheless retains the communications on the vehicle’s on-board memory, even after the cellphone is disconnected. Vehicle owners cannot access or delete their personal information once it has been stored,” the ruling’s summary of the complaint said.

Products can extract messages and call logs

Ford’s website provides instructions for a factory reset that “erases all stored data, such as call history, text messages, previously paired phones,” and other data. That’s useful before one sells or transfers a car but doesn’t allow drivers to manually delete specific messages or call logs while they’re still using the vehicle with a connected phone.

There was no allegation that Ford or the other carmakers directly accessed text messages or call logs, or that they stored the data in their own systems. The privacy concern comes from the fact that a company called Berla sells specialized data-retrieval products to law enforcement, which could use the products to obtain messages and logs from a car.

Berla's website boasts that "having access to a suspect's connected vehicle is the next best thing behind having the actual phone itself." In a statement quoted in the plaintiffs' complaint, Berla also says that if "a driver uses the infotainment interface to 'delete' their device, that device information often remains in unallocated space and can be recovered."

"According to the Plaintiffs, Berla produces hardware and software capable of extracting stored text messages and call logs stored on a vehicle's on-board memory," the appeals court ruling said. "Berla products are not generally available to the public, and sales access is restricted to law enforcement, the military, civil and regulatory agencies, and select private investigation service providers."

https://arstechnica.com/?p=1982702

Google, Meta, TikTok defeat Austria's plan to combat hate speech

reader comments

34 with

On Thursday, a top European court ruled that Austria cannot force Google, Meta, and TikTok to pay millions in fines if

they fail to delete hate speech from their popular social media platforms.

Austria had attempted to hold platforms accountable for hate speech and other illegal content after passing a law in 2021 requiring tech giants to publish reports as often as every six months detailing content takedowns. Like the European Union's recently adopted Digital Services Act, the Austrian law sought to impose fines—up to $10.69 million, Reuters reported—for failing to tackle illegal or harmful content.

However, soon after Austria tried to enforce the law, Google, Meta, and TikTok—each with EU operations based in Ireland—challenged it in an Austrian court. The tech companies insisted that Austria's law conflicted with an EU law that says that platforms are only subject to laws in EU member states where they're established.

Because there is still plenty of legal uncertainty as to how EU member states can regulate services originating from other member states, the Austrian court asked the Court of Justice of the European Union (CJEU) to weigh in.

Advertisement

Ultimately, the CJEU agreed with tech companies, deciding that the language of Austria's law was too general and abstract, potentially applying to too many platforms without distinction. The court ruling said that allowing Austria to enforce the law risked restricting "the free movement of information society services" between EU member states and undermining "mutual trust" between member states.

The ruling represented a major victory for platforms attempting to comply with ever-stricter user protections recently enforceable in the EU. According to Reuters, CJEU's ruling cannot be appealed. Next, the Austrian court will conclude its legal proceedings, likely sealing the win for platforms and setting an important precedent that could shield

platforms from other potential legal attacks as EU regulators continue to crack down on Big Tech.

Meta and TikTok did not immediately respond to Ars' request to comment on the ruling, but a Google spokesperson confirmed that the judgment will inform how Google's trust and safety efforts are managed in the EU.

"We are pleased with today's decision, which reaffirms the importance of the EU's country of origin principle," Google's spokesperson told Ars. "We will study the judgment and continue to invest in the trust and safety of our users across our platforms."

https://arstechnica.com/?p=1982631

AirTags are the new go-to tool for cops after spike in car thefts

reader comments

28 with

After a viral TikTok trend spurred tens of thousands of car thefts this summer, cops in Washington, DC, started realizing that it was much easier to recover stolen vehicles that could be tracked with Apple AirTags.

Because of this, the Metropolitan Police Department (MPD) rolled out a pilot program this week, doling out free tracking devices to residents in DC areas where cops are seeing “the greatest increase in vehicle theft,” according to a press release from the office of DC mayor Muriel Bowser.

Over the next few days, MPD will hand out the tracking devices—both AirTags and Tiles—at distribution events, where officers will help residents hide the devices in their vehicles and pair the devices to their phones. Residents will be able to choose whether they want an AirTag or a Tile, MPD said, and once the device is installed, only the resident will have access to tracking information as the sole owner of the device, but they will be required to share data with police if their vehicle is stolen.

“Our goal is not just to prevent carjackings and motor vehicle thefts, but also to ensure swift law enforcement action when these incidents occur,” Pamela Smith, MPD’s acting chief of police, said in the press release. “These tracking devices allow our officers and detectives to be better positioned to quickly locate stolen vehicles, recover property, and gather vital evidence for investigations.”

Advertisement

At a press conference, Smith declined to say how many tracking devices would be distributed to DC residents, but she noted that more than 1,000 residents signed up for a wheel lock distribution program similarly designed to prevent car thefts. At the same event, Bowser said that “thousands” of residents signed up for a Private Security Camera Incentive Program, receiving a $500 rebate after installing security cameras outside their homes or businesses.

While MPD made it clear that “the device can only be accessed by the owner of the device,” the price of participating in the pilot seems to be a promise to cooperate with law enforcement if a resident’s car is ever stolen.

“Participating in the program means you are pledging to share tracking data if your vehicle is stolen at a future date,” MPD said in an FAQ. That specifically means that residents are agreeing to “log into your account and show the officer where your device is pinging,” should their car get stolen.

This could raise privacy concerns for some residents who might want to better understand how their data could be used by police before participating in the program. A spokesperson for the Electronic Frontier Foundation (EFF), a nonprofit digital rights group, told Ars that “people have every right to opt into this, but they should be fully informed and that means asking questions about the exact terms that apply—for example, what the AirTag and Tile policies are regarding release of user data to law enforcement.”

https://arstechnica.com/?p=1982442

Internet providers say the FCC should not investigate broadband prices

Getty Images | traffic_analyzer

reader comments

49 with

Internet service providers and their lobby groups are fighting a US plan to prohibit discrimination in access to broadband

services. In particular, ISPs want the Federal Communications Commission to drop the plan's proposal to require that prices charged to consumers be non-discriminatory.

In 2021, Congress required the Federal Communications Commission to issue rules "preventing digital discrimination of access based on income level, race, ethnicity, color, religion, or national origin" within two years. FCC Chairwoman Jessica Rosenworcel last month released her draft plan to comply with the congressional mandate and scheduled a November 15 commission vote on adopting final rules.

The plan is likely to pass in a party-line vote as Rosenworcel has a 3-2 Democratic majority, but aspects of the draft could be changed before the vote. Next week's meeting could be a contentious one, judging by a statement issued Monday by Republican Commissioner Brendan Carr.

Carr described Rosenworcel's proposal as "President Biden's plan to give the administrative state effective control of all Internet services and infrastructure in the US." He also objects to the Rosenworcel plan's statement that the FCC rules may apply to entities that are not broadband providers, such as landlords, if they "impede equal access to broadband Internet access service."

Consumer advocates generally support the proposal but say the planned system for handling complaints, ISP responses, and investigations is not transparent enough, reducing the system's potential to act as a deterrent. Consumer advocates also say Internet users who have already been harmed by discrimination may not get any relief because the proposed rules do not apply retroactively.

ISPs: Don't investigate our prices

ISPs including Comcast, Charter, AT&T, and Verizon have held a flurry of meetings with FCC officials and commissioners in

which they argued that the rules are too broad. The broadband firms are especially concerned about the FCC's plan to consider the prices consumers pay when determining whether an ISP practice is discriminatory. The industry wants the FCC to consider only the deployment of broadband, not other factors such as how much it costs.

Advertisement

In a meeting with Rosenworcel's staff, cable company executives "stated that the Draft Order would impose overbroad liability standards that impede further broadband investment and are legally vulnerable by adopting a disparate impact rather than a disparate treatment liability approach," according to an ex parte filing submitted yesterday by cable lobby group NCTA-The Internet & Television Association. The meeting included executives from Comcast, Charter, and Cox.

The cable companies said the FCC "should define digital discrimination as disparate treatment and should limit the standard to policies and practices involving the deployment of broadband network facilities. It should not regulate rates or non-technical aspects of broadband service." The cable industry filing said "it is especially important for the Commission to exclude 'price' from the list of 'covered elements of service.'"

Similar arguments were raised by wireless industry trade group CTIA. "Evaluating matters such as pricing, deposits, discounts, and data caps *is* price regulation because the Commission may levy consequences based on the price per level of service that a provider chooses to offer," CTIA said. "Commission evaluation of price is unnecessary in the competitive wireless marketplace and may deter offering discounts and enticements to switch providers that consumers enjoy today."

More opposition came in filings submitted by AT&T, Verizon, and the USTelecom industry group. ISPs and their trade groups

will likely sue the FCC if the rules are approved.

“The draft rules ignore the statute’s clear focus on broadband deployment and instead cast a net so wide it would capture every business decision a provider makes concerning how to sell its product, with little regard to the reasonableness (or usefulness) of that decision,” AT&T said. “This regulatory overreach will impose unnecessary regulation on broadband providers and divert attention and vital resources from broadband investment and deployment at this key juncture in the bipartisan Infrastructure Act’s Broadband, Equity, Access & Deployment Program (BEAD).” That’s a reference to a $42 billion grant program that will pay ISPs to expand their networks.

ISPs previously complained about an unrelated rule requiring them to list all their monthly fees, but the FCC rejected their complaints and issued the rule.

https://arstechnica.com/?p=1982368

Data broker’s “staggering” sale of sensitive info exposed in unsealed FTC filing

reader comments

44 with

One of the world’s largest mobile data brokers, Kochava, has lost its battle to stop the Federal Trade Commission from revealing what the FTC has alleged is a disturbing, widespread pattern of unfair use and sale of sensitive data without consent from hundreds of millions of people.

US District Judge B. Lynn Winmill recently unsealed a court filing, an amended complaint that perhaps contains the most evidence yet gathered by the FTC in its long-standing mission to crack down on data brokers allegedly “substantially” harming consumers by invading their privacy.

The FTC has accused Kochava of violating the FTC Act by amassing and disclosing “a staggering amount of sensitive and identifying information about consumers,” alleging that Kochava’s database includes products seemingly capable of identifying nearly every person in the United States.

According to the FTC, Kochava’s customers, ostensibly advertisers, can access this data to trace individuals’ movements—including to sensitive locations like hospitals, temporary shelters, and places of worship, with a promised accuracy within “a few meters”—over a day, a week, a month, or a year. Kochava’s products can also provide a “360-degree perspective” on individuals, unveiling personally identifying information like their names, home addresses, phone numbers, as well as sensitive information like their race, gender, ethnicity, annual income, political affiliations, or religion, the FTC alleged.

Beyond that, the FTC alleged that Kochava also makes it easy for advertisers to target customers by categories that are “often based on specific sensitive and personal characteristics or attributes identified from its massive

collection of data about individual consumers." These "audience segments" allegedly allow advertisers to conduct invasive targeting by grouping people not just by common data points like age or gender, but by "places they have visited," political associations, or even their current circumstances, like whether they're expectant parents. Or advertisers can allegedly combine data points to target highly specific audience segments like "all the pregnant Muslim women in Kochava's database," the FTC alleged, or "parents with different ages of children."

Advertisement

"Kochava's use and disclosure of this precise geolocation information invade consumers' privacy and cause or are likely to cause consumers substantial injury," the FTC's amended complaint said. "In addition, Kochava collects, uses, and discloses enormous amounts of additional private and sensitive information about consumers. Kochava's use and disclosure of this data, whether alone or in conjunction with Kochava's geolocation data, also invade consumers' privacy and cause or are likely to cause consumers substantial injury."

According to the FTC, Kochava obtains data "from a myriad of sources, including from mobile apps and other data brokers," which together allegedly connects a web of data that "contains information about consumers' usage of over 275,000 mobile apps."

The FTC alleged that this usage data is also invasive, allowing Kochava customers to track not just what apps a customer uses, but how long they've used the apps, what they do in the apps, and how much money they spent in the apps, the FTC alleged.

Kochava "provides an unprecedented view into a consumer's personal actions, decisions, and behaviors," the FTC alleged, seeming particularly concerned that Kochava collects barely any information from its customers before providing access to

this sensitive information. “Kochava’s practices intrude into the most private areas of consumers’ lives and cause or are likely to cause substantial injury to consumers,” the complaint said.

Kochava “could implement safeguards to protect consumer privacy, such as blacklisting sensitive locations from its data feeds or removing sensitive characteristics from its data” at “a reasonable cost and expenditure of resources,” but deliberately chooses not to, the FTC alleged. Instead, Kochava “actively promotes its data as a means to evade consumers’ privacy choices,” the FTC alleged. Further, the FTC alleged that there are no real ways for consumers to opt out of Kochava’s data marketplace, because even resetting their mobile advertising IDs—the data point that’s allegedly most commonly used to identify users in its database—won’t stop Kochava customers from using its products to determine “other points to connect to and securely solve for identity.”

https://arstechnica.com/?p=1982106