# Big loss for ISPs as Supreme Court won’t hear challenge to $15 broadband law

The Supreme Court petition was filed by the New York State Telecommunications Association, CTIA-The Wireless Association, NTCA-The Rural Broadband Association, USTelecom, ACA Connects-America’s Communications Association, and the Satellite Broadcasting and Communications Association. Cable lobby group NCTA filed a brief supporting the petition.

New York Attorney General Letitia James defended the state law in a Supreme Court brief filed in October. The brief said that when New York enacted its law, the Pai-era FCC “had classified broadband as an information service subject to Title I of the Communications Act. Under Title I, Congress gave the FCC only limited regulatory authority—leaving ample room for States to regulate information services.”

Multiple appeals courts have found “that federal law does not broadly preempt state regulations of Title I information services,” and “Congress has expressed no intent—much less the requisite clear and manifest intent—to preempt state regulation of Title I information services,” the New York brief said. “Applicants’ field preemption claim fails because, far from imposing a pervasive federal regulatory regime on Title I information services, Congress instead gave the FCC only limited authority over information services. Congress thus left the States’ traditional police powers over information services largely untouched.”

# Law requires $15 price, or $20 for higher speeds

It’s unclear when New York might start enforcing its law. The state law was approved in 2021 and required ISPs to offer $15 broadband plans with download speeds of at least 25Mbps, with the $15 being “inclusive of any recurring taxes and fees such as recurring rental fees for service provider equipment required to obtain broadband service and usage fees.”

The law also said ISPs could instead choose to comply by offering $20-per-month service with 200Mbps speeds. Price increases would be capped at 2 percent per year, and state officials would periodically review whether minimum required speeds should be raised.

Residents who meet income eligibility requirements would qualify for the plans. ISPs with 20,000 or fewer subscribers would be allowed to apply for exemptions from the law.

The New York attorney general’s Supreme Court brief argued that public-interest factors “weigh heavily in favor of allowing” the law, and that it won’t create the economic problems that telco groups warned of. “The three largest broadband providers in New York are already offering an affordable broadband product to low-income consumers irrespective of the ABA, and smaller broadband providers can seek an exemption from the ABA’s requirements,” the brief said.

https://arstechnica.com/tech-policy/2024/12/big-loss-for-isps-as-supreme-court-wont-hear-challenge-to-15-broadband-law/

# Facing ban next month, TikTok begs SCOTUS for help

## TikTok: Ban is slippery slope to broad US censorship

According to TikTok, the government's defense of the ban to prevent China from wielding a "covert" influence over Americans is a farce invented by lawyers to cover up the true mission of censorship. If the lower court's verdict stands, TikTok alleged, "then Congress will have free rein to ban any American from speaking simply by identifying some risk that the speech is influenced by a foreign entity."

TikTok doesn't want to post big disclaimers on the app warning of "covert" influence, claiming that the government relied on "secret evidence" to prove this influence occurs on TikTok. But if the Supreme Court agrees that the government needed to show more than "bare factual assertions" to back national security claims the lower court said justified any potential speech restrictions, then the court will also likely agree to reverse the lower court's decision, TikTok suggested.

It will become much clearer by January 6 whether the January 19 ban will take effect, at which point TikTok would shut down, booting all US users from the app. TikTok urged the Supreme Court to agree it is in the public interest to delay the ban and review the constitutional claims to prevent any "extreme" harms to both TikTok and US users who depend on the app for news, community, and income.

If SCOTUS doesn't intervene, TikTok said that the lower

court’s “flawed legal rationales would open the door to upholding content-based speech bans in contexts far different than this one.”

“Fearmongering about national security cannot obscure the threat that the Act itself poses to all Americans,” TikTok alleged, while suggesting that even Congress would agree that a “modest delay” in enforcing the law wouldn’t pose any immediate risk to US national security. Congress is also aware that a sale would not be technically, commercially, or legally possible in the timeframe provided, TikTok said. A temporary injunction would prevent irreparable harms, TikTok said, including the irreparable harm courts have long held is caused by restricting speech of Americans for any amount of time.

“An interim injunction is also appropriate because it will give the incoming Administration time to determine its position, as the President-elect and his advisors have voiced support for saving TikTok,” TikTok argued.

Ars could not immediately reach TikTok for comment.

https://arstechnica.com/tech-policy/2024/12/facing-ban-next-month-tiktok-begs-scotus-for-help/

---

# In IT? Need cash? Cybersecurity whistleblowers are earning big payouts.

Matthew Decker is the former chief information officer for

Penn State University's Applied Research Laboratory. As of October, he's also $250,000 richer.

In his Penn State position, Decker was well placed to see that the university was not implementing all of the cybersecurity controls that were required by its various contracts with NASA and the Department of Defense (DoD). It did not, for instance, use an external cloud services provider that met the DoD's security guidelines, and it fudged some of the self-submitted "scores" it made to the government about Penn State's IT security.

So Decker sued the school under the False Claims Act, which lets private individuals bring cases against organizations on behalf of the government if they come across evidence of wrongdoing related to government contracts. In many of these cases, the government later "intervenes" to assist with the case (as it did here), but whether it does so or not, whistleblowers stand to collect a percentage of any fines if they win.

In October, Penn State agreed to a $1.25 million settlement with the government; Decker got $250,000 of the money.

## On the regular

This now happens in IT with some regularity. In November, Dell, Dell Federal Systems, and Iron Bow Technologies settled with the government for $4.3 million over claims that they "violated the False Claims Act by submitting and causing the submission of non-competitive bids to the Army and thereby overcharging the Army under the Army Desktop and Mobile Computing 3 (ADMC-3) contract."

But once again, this wasn't something the government uncovered on its own; a whistleblower named Brent Lillard, who was an executive at another company in the industry, brought the initial complaint. For his work, Lillard just made $345,000.

In early December, Gen Digital (formerly Symantec) paid a much larger fee—$55.1 million—after losing a trial in 2022. Gen Digital/Symantec was found liable for charging the government higher prices than it charged to companies.

Once again, the issue was brought to light by a whistleblower, Lori Morsell, who oversaw the contract for Gen Digital/Symantec. Morsell's award has not yet been determined by the court, but given the amount of the payout, it should be substantial.

## False Claims Act goes digital

Due to the complexity of investigating—or even finding out about—technical failures and False Claims Act cases from the outside of an organization, the government has increasingly relied on whistleblowers to kick-start these sorts of IT cases.

https://arstechnica.com/tech-policy/2024/12/in-it-need-cash-cybersecurity-whistleblowers-are-earning-big-payouts/

---

# Character.AI steps up teen safety after bots allegedly caused suicide, self-harm

Following a pair of lawsuits alleging that chatbots caused a teen boy's suicide, groomed a 9-year-old girl, and caused a vulnerable teen to self-harm, Character.AI (C.AI) has

announced a separate model just for teens, ages 13 and up, that’s supposed to make their experiences with bots safer.

In a blog, C.AI said it took a month to develop the teen model, with the goal of guiding the existing model “away from certain responses or interactions, reducing the likelihood of users encountering, or prompting the model to return, sensitive or suggestive content.”

C.AI said “evolving the model experience” to reduce the likelihood kids are engaging in harmful chats—including bots allegedly teaching a teen with high-functioning autism to self-harm and delivering inappropriate adult content to all kids whose families are suing—it had to tweak both model inputs and outputs.

To stop chatbots from initiating and responding to harmful dialogs, C.AI added classifiers that should help C.AI identify and filter out sensitive content from outputs. And to prevent kids from pushing bots to discuss sensitive topics, C.AI said that it had improved “detection, response, and intervention related to inputs from all users.” That ideally includes blocking any sensitive content from appearing in the chat.

Perhaps most significantly, C.AI will now link kids to resources if they try to discuss suicide or self-harm, which C.AI had not done previously, frustrating parents suing who argue this common practice for social media platforms should extend to chatbots.

## Other teen safety features

In addition to creating the model just for teens, C.AI announced other safety features, including more robust parental controls rolling out early next year. Those controls would allow parents to track how much time kids are spending on C.AI and which bots they’re interacting with most frequently, the blog said.

C.AI will also be notifying teens when they've spent an hour on the platform, which could help prevent kids from becoming addicted to the app, as parents suing have alleged. In one case, parents had to lock their son's iPad in a safe to keep him from using the app after bots allegedly repeatedly encouraged him to self-harm and even suggested murdering his parents. That teen has vowed to start using the app whenever he next has access, while parents fear the bots' seeming influence may continue causing harm if he follows through on threats to run away.

https://arstechnica.com/tech-policy/2024/12/character-ai-steps-up-teen-safety-after-bots-allegedly-caused-suicide-self-harm/

---

# Report: AT&T, Verizon aren't notifying most victims of Chinese call-records hack

Telecom companies aren't required to notify customers about every breach. A Federal Communications Commission order in December 2023 adopted a "harm-based notification trigger" in which "notification of a breach to consumers is not required in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed."

The FCC said that harm requiring notifications can include,

but is not limited to, “financial harm, physical harm, identity theft, theft of services, potential for blackmail, the disclosure of private facts, the disclosure of contact information for victims of abuse, and other similar types of dangers.”

The FCC order argued that the harm-based standard would let carriers “focus their time, effort, and financial resources on the most important and potentially harmful incidents” and protect “customers from over-notification and notice fatigue, specifically in instances where the carrier has reasonably determined that no harm is likely to occur.”

## Senator: Telecoms should tell customers

US Sen. Ron Wyden (D-Ore.) this week criticized the carriers for having weak security and the FCC for “let[ting] phone companies write their own cybersecurity rules.” Wyden proposed legislation to beef up telecom security requirements.

A spokesperson for Wyden today said that carriers should notify the affected customers.

“Senator Wyden strongly supports the phone companies notifying their customers about the theft of their data,” the spokesperson told Ars. “Not only do Americans have a right to be told that their information was stolen, but this is useful information that could result in some consumers voting with their wallets and switching service to carriers that retain less data and or have better cybersecurity.”

Stanford University researchers collected and studied telephone metadata for a 2016 paper to determine how it could be used against customers. “Using crowdsourced telephone logs and social networking information, we find that telephone metadata is densely interconnected, susceptible to

reidentification, and enables highly sensitive inferences," they wrote.

https://arstechnica.com/tech-policy/2024/12/report-att-verizon-arent-notifying-most-victims-of-chinese-call-records-hack/

---

# Photobucket opted inactive users into privacy nightmare, lawsuit says

Photobucket was sued Wednesday after a recent privacy policy update revealed plans to sell users' photos—including biometric identifiers like face and iris scans—to companies training generative AI models.

The proposed class action seeks to stop Photobucket from selling users' data without first obtaining written consent, alleging that Photobucket either intentionally or negligently failed to comply with strict privacy laws in states like Illinois, New York, and California by claiming it can't reliably determine users' geolocation.

Two separate classes could be protected by the litigation. The first includes anyone who ever uploaded a photo between 2003—when Photobucket was founded—and May 1, 2024. Another potentially even larger class includes any non-users depicted in photographs uploaded to Photobucket, whose biometric data has also allegedly been sold without consent.

Photobucket risks huge fines if a jury agrees with Photobucket

users that the photo-storing site unjustly enriched itself by breaching its user contracts and illegally seizing biometric data without consent. As many as 100 million users could be awarded untold punitive damages, as well as up to $5,000 per “willful or reckless violation” of various statutes.

If a substantial portion of Photobucket’s entire 13 billion-plus photo collection is found infringing, the fines could add up quickly. In October, Photobucket estimated that “about half of its 13 billion images are public and eligible for AI licensing,” Business Insider reported.

Users suing include a mother of a minor whose biometric data was collected and a professional photographer in Illinois who should have been protected by one of the country’s strongest biometric privacy laws.

So far, Photobucket has confirmed that at least one “alarmed” Illinois user’s data may have already been sold to train AI. The lawsuit alleged that most users eligible to join the class action likely similarly only learned of the “conduct long after the date that Photobucket began selling, licensing, and/or otherwise disclosing Class Members’ biometric data to third parties.”

https://arstechnica.com/tech-policy/2024/12/photobucket-sold-users-biometric-data-without-consent-lawsuit-says/

---

# Report: Google told FTC Microsoft’s OpenAI deal is

# killing AI competition

Google reportedly wants the US Federal Trade Commission (FTC) to end Microsoft's exclusive cloud deal with OpenAI that requires anyone wanting access to OpenAI's models to go through Microsoft's servers.

Someone "directly involved" in Google's effort told The Information that Google's request came after the FTC began broadly probing how Microsoft's cloud computing business practices may be harming competition.

As part of the FTC's investigation, the agency apparently asked Microsoft's biggest rivals if the exclusive OpenAI deal was "preventing them from competing in the burgeoning artificial intelligence market," multiple sources told The Information. Google reportedly was among those arguing that the deal harms competition by saddling rivals with extra costs and blocking them from hosting OpenAI's latest models themselves.

In 2024 alone, Microsoft generated about $1 billion from reselling OpenAI's large language models (LLMs), The Information reported, while rivals were stuck paying to train staff to move data to Microsoft servers if their customers wanted access to OpenAI technology. For one customer, Intuit, it cost millions monthly to access OpenAI models on Microsoft's servers, The Information reported.

Microsoft benefits from the arrangement—which is not necessarily illegal—of increased revenue from reselling LLMs and renting out more cloud servers. It also takes a 20 percent cut of OpenAI's revenue. Last year, OpenAI made approximately $3 billion selling its LLMs to customers like T-Mobile and Walmart, The Information reported.

Microsoft’s agreement with OpenAI could be viewed as anti-competitive if businesses convince the FTC that the costs of switching to Microsoft’s servers to access OpenAI technology is so burdensome that it’s unfairly disadvantaging rivals. It could also be considered harming the market and hampering innovation by seemingly disincentivizing Microsoft from competing with OpenAI in the market.

To avoid any disruption to the deal, however, Microsoft could simply point to AI models sold by Google and Amazon as proof of “robust competition,” The Information noted. The FTC may not buy that defense, though, since rivals’ AI models significantly fall behind OpenAI’s models in sales. Any perception that the AI market is being foreclosed by an entrenched major player could trigger intense scrutiny as the US seeks to become a world leader in AI technology development.

https://arstechnica.com/tech-policy/2024/12/report-microsofts-exclusive-deal-with-openai-harms-competition-google-told-ftc/

---

# Micron’s $6B CHIPS funding should have more strings attached, critics say

# Advocates: Micron needs to explain what a “good job” is

But while Neuffer joined Harris’ and the Commerce Department’s chorus, praising the award for creating “high-paying American jobs,” bolstering US national and economic security, and fueling “innovation for years to come,” communities are raising questions.

Advocates with Jobs to Move America (JMA)—who are organizing ahead of Micron’s New York construction starting in 2026—are concerned that Micron hasn’t been clear about what a “good job” is before moving into an area with “one of the highest poverty rates in the country.”

“There has been little discussion or firm commitments made regarding what exactly a ‘good job’ is, or how equitable access for said jobs will be achieved for current local residents,” JMA’s “Good Jobs Platform,” drafted earlier this year with more than 20 local advocacy groups, said.

“We define a ‘good job’ as one that guarantees: workers have a fair and clear process to organize a union without employer opposition, family-sustaining wages and comprehensive benefits, safe working conditions, equitable hiring and employment practices, and is supported by an accessible workforce pipeline,” the platform said.

And equally important are communities’ and workers’ health and safety concerns, the platform noted, urging that “a good job is a safe job.”

A senior researcher and policy coordinator for JMA, Anna Smith, told Ars that Harris’ statement was missing any mention of a community impact statement. And while Harris mentioned “utilizing project labor agreements and registered apprenticeship programs, which will further strengthen local economies” and “support workers,” more enforceable commitments

are needed to protect communities as Micron’s construction begins, Smith said.

The “Good Jobs Platform” recommends a range of commitments, from labor peace agreements that would ensure workers can unionize to community workforce agreements keeping workers involved in key discussions regarding ongoing training and career development. Local labor leaders have sought similar commitments, urging Micron to commit to a community benefits agreement “that enshrines legally enforceable provisions that protect the community, its workers, and the environment.”

https://arstechnica.com/tech-policy/2024/12/microns-6b-chips-funding-should-have-more-strings-attached-critics-say/

---

# Location data firm helps police find out when suspects visited their doctor

The intake form “was included in an email thread between a Fog representative and Bryan Kimbell, chief human trafficking investigator at the Office of the Attorney General in Georgia,” according to 404 Media.

Services like Fog Data Science have triggered concerns about how police might use location tracking to prosecute abortions. “For several thousand dollars annually, the software lets police trace unique borders around large, customized regions to generate a list of devices in the area. Police can use Fog

Reveal to geofence entire buildings or street blocks—like the area surrounding an abortion clinic—and get information on devices used within and surrounding those buildings to identify suspects," Ars wrote in November 2022.

The EFF's 2022 investigation found that Fog obtained data from the firm Venntel, which is the subject of a Federal Trade Commission action. The FTC last week announced a proposed settlement with Venntel and its owner, Gravy Analytics. The FTC alleged that "Gravy Analytics and Venntel violated the FTC Act by unfairly selling sensitive consumer location data, and by collecting and using consumers' location data without obtaining verifiable user consent for commercial and government uses."

"Surreptitious surveillance by data brokers undermines our civil liberties and puts servicemembers, union workers, religious minorities, and others at risk," Samuel Levine, director of the FTC Bureau of Consumer Protection, said in the announcement. According to the FTC, Gravy Analytics used geofencing "to identify and sell lists of consumers who attended certain events related to medical conditions and places of worship and sold additional lists that associate individual consumers to other sensitive characteristics."

If the proposed order takes effect, "Gravy Analytics and Venntel will be prohibited from selling, disclosing, or using sensitive location data in any product or service, and must establish a sensitive data location program," the FTC said. One of the FTC's two Republicans partially dissented from the decision, which may not be finalized until after President-elect Trump takes office.

https://arstechnica.com/tech-policy/2024/12/location-data-firm-helps-police-find-out-when-suspects-visited-their-doctor/

# Apple hit with $1.2B lawsuit after killing controversial CSAM-detecting tool

When Apple devices are used to spread CSAM, it's a huge problem for survivors, who allegedly face a range of harms, including "exposure to predators, sexual exploitation, dissociative behavior, withdrawal symptoms, social isolation, damage to body image and self-worth, increased risky behavior, and profound mental health issues, including but not limited to depression, anxiety, suicidal ideation, self-harm, insomnia, eating disorders, death, and other harmful effects." One survivor told The Times she "lives in constant fear that someone might track her down and recognize her."

Survivors suing have also incurred medical and other expenses due to Apple's inaction, the lawsuit alleged. And those expenses will keep piling up if the court battle drags on for years and Apple's practices remain unchanged.

Apple could win, a lawyer and policy fellow at the Stanford Institute for Human-Centered Artificial Intelligence, Riana Pfefferkorn, told The Times, as survivors face "significant hurdles" seeking liability for mishandling content that Apple says Section 230 shields. And a win for survivors could "backfire," Pfefferkorn suggested, if Apple proves that forced scanning of devices and services violates the Fourth Amendment.

Survivors, some of whom own iPhones, think that Apple has a

responsibility to protect them. In a press release, Margaret E. Mabie, a lawyer representing survivors, praised survivors for raising “a call for justice and a demand for Apple to finally take responsibility and protect these victims.”

“Thousands of brave survivors are coming forward to demand accountability from one of the most successful technology companies on the planet,” Mabie said. “Apple has not only rejected helping these victims, it has advertised the fact that it does not detect child sex abuse material on its platform or devices thereby exponentially increasing the ongoing harm caused to these victims.”

https://arstechnica.com/tech-policy/2024/12/thousands-of-child-sex-abuse-victims-sue-apple-for-lax-csam-reporting/