French parliament passes porn age-verification legislation

Enlarge / French President Emmanuel Macron.
LUDOVIC MARIN/POOL/AFP via Getty Images

reader comments

148 with 96 posters participating

Share this story

The French parliament has agreed to pass a new law requiring age verification on pornographic websites to prevent access by children under 18, Politico reports. The initiative has the support of President Emmanuel Macron, who called for such a measure in January.

The French law gives sites discretion to decide how to perform age verification. Requiring users to enter a credit card number seems to be one of the most popular options.

According to Politico, the law gives French regulators the power to create a blacklist for overseas sites that don't comply with the new rules. If a site doesn't respond to a warning from French officials, they can "ask the Paris Court of Justice to send an order to telecom operators to block the access to these sites from France."

France is one of several countries considering legislation to keep pornography away from children. In the United Kingdom, the government has been trying for several years to establish a system for age-verifying porn sites. That effort hasn't gone well. After multiple delays, the government put the effort on hold indefinitely last October. Australian legislators are

considering a similar measure.

A major sticking point in the UK's age verification debate was privacy. Critics pointed out that it wasn't a great idea to force adult consumers to turn over their credit card numbers to porn sites that might not have the strongest privacy protections—or the highest ethical standards. It's not clear what privacy protections will be offered to consumers under the French law.

https://arstechnica.com/?p=1690741

Frontier misled subscribers about Internet speeds and prices, AG finds

Enlarge / A Frontier Communications service van.

reader comments

69 with 58 posters participating

Share this story

Frontier Communications misled thousands of customers about the prices it charges and about the speeds its broadband network can provide, Washington State Attorney General Bob Ferguson's office has found.

The state's investigation of Frontier's business practices

found evidence of the telecom “failing to adequately disclose taxes and fees during sales of cable, Internet, and telephone services; failing to adequately disclose its Internet Infrastructure Surcharge fee in advertising; misleading consumers by implying that the Internet Infrastructure Surcharge and other fees are mandatory and/or government-related fees; and misleading consumers as to Internet speeds it could offer, and failing to deliver speeds and service as advertised.”

The findings are described in a settlement that will force Frontier Communications to pay a $900,000 fine and force the new owner of Frontier’s network in Washington state to change its business practices. Among other things, the settlement requires Frontier’s current owner in Washington to stop charging the $3.99-per-month Internet Infrastructure Surcharge. The company “neither admits nor denies the State’s findings.” The settlement still needs court approval before it can take effect.

The offending business practices began before Frontier Communications’ May 2020 sale of its operations in Washington, Oregon, Idaho, and Montana to Northwest Fiber, also known as Ziply Fiber. The settlement document refers to the company as both “Frontier Communications” and “Frontier Northwest.” The company has about 165,000 Internet customers in Washington state, mostly in rural areas.

Frontier Communications itself still operates in 25 other states; the company filed for bankruptcy in April.

Under the pending settlement, Frontier Northwest “is ordered to clearly and conspicuously disclose all fees,” Ferguson said in an announcement yesterday. “To resolve Ferguson’s investigation, Frontier Northwest is also required to be transparent about its available Internet speeds. The Attorney [General’s] Office will set aside the majority of the $900,000 payment to provide restitution to impacted customers.” The

proposed settlement was filed in Thurston County Superior Court.

Customers who were overcharged need to wait a bit before getting refunds, as Ferguson's office said it "will announce details of the claims process when they are finalized."

Ferguson previously forced CenturyLink to pay a $6.1 million penalty after finding that the company failed to disclose fees that raised actual prices well above the advertised rates. That settlement forced CenturyLink to stop charging its so-called "Internet Cost Recovery Fee" in the state.

Investigation began in 2018

Ferguson began investigating Frontier in 2018 after receiving more than 600 complaints and "focused on Frontier Northwest's failure to adequately disclose fees during sales of cable, Internet and phone services since 2016," Ferguson's announcement said. "For example, the company charged as much as $3.99—nearly $50 per year—for an 'Internet Infrastructure Surcharge,' without adequately disclosing the surcharge in its advertising."

After the settlement is approved, Frontier Northwest will be required to clearly disclose the following to customers in Washington state:

- *The monthly base price of the services*
- *The estimated amount of taxes, fees, or other recurring charges for the services*
- *The amount of each one-time fee, or fee charged only on the customer's first invoice, for the purchased services, including activation and installation fees and equipment purchases*
- *Any applicable cancellation or termination fees*

“Within three business days after a sale, Frontier must send the customer an order confirmation that clearly sets forth the pricing and terms and conditions of service” and give the customer an opportunity to make changes, Ferguson’s office said.

The settlement calls for conditions to remain in effect for 10 years, a time period that could be extended “in the event of noncompliance.”

Unfortunately for customers, the settlement’s requirement to stop charging the Internet Infrastructure Surcharge doesn’t take effect right away. Frontier Northwest is required to stop charging the fee to new customers within 90 days of the settlement taking effect. But for existing customers, Frontier Northwest will have a full year after the settlement’s effective date before it has to discontinue the charge.

For new customers, Frontier Northwest will not be allowed to charge cancellation or unreturned-equipment fees unless it disclosed those fees when the customer initially bought the service.

As far as advertised broadband speeds, the settlement says that “Frontier shall make clear and conspicuous disclosures that comply with applicable Federal Trade Commission guidelines and Washington Iaw.”

To complete its purchase of Frontier’s network, the new owner previously committed to invest $50 million to improve and expand fiber and provide gigabit-speed fiber service to 33 percent of the company’s customer locations in Washington state within five years. The pending settlement announced yesterday would add additional advertising and speed-disclosure requirements that would be triggered if Frontier Northwest fails to meet the $50 million commitment.

https://arstechnica.com/?p=1690487

Microsoft neuters Office 365 account attacks that used clever ruse

reader comments

21 with 18 posters participating

Share this story

Microsoft has neutered a large-scale fraud campaign that used knock-off domains and malicious apps to scam customers in 62 countries around the world.

The software maker and cloud-service provider last week obtained a court order that allowed it to seize six domains, five of which contained the word “office.” The company said attackers used them in a sophisticated campaign designed to trick CEOs and other high-ranking business leaders into wiring large sums of money to attackers, rather than trusted parties. An earlier so-called BEC, or business email compromise, that the same group of attackers carried out in December used phishing attacks to obtain unauthorized access. The emails used generic business themes such as quarterly earnings reports. Microsoft used technical means to shut it down.

The attackers returned with a new BEC that took a different tack: instead of tricking targets into logging in to lookalike sites, and consequently divulging the passwords, the scam used

emails that instructed the recipient to give what was purported to be a Microsoft app access to an Office 365 account. The latest scam used the COVID-19 pandemic as a lure.

“This scheme enabled unauthorized access without explicitly requiring the victims to directly give up their login credentials at a fake website or similar interface, as they would in a more traditional phishing campaign,” Tom Burt, Microsoft’s Corporate Vice President for Customer Security & Trust, wrote. “After clicking through the consent prompt for the malicious web app (pictured below), the victim unwittingly granted criminals permission to access and control the victims’ Office 365 account contents, including email, contacts, notes and material stored in the victims’ OneDrive for Business cloud storage space and corporate SharePoint document management and storage system.”

Burt cited a 2019 report from the FBI that said BEC crimes caused losses of more than $1.7 billion, almost half of all financial losses caused by Internet crime. BECs were the most costly complaint received by the Internet Crime Center, according to the report. In some of the more well-executed campaigns, executives receive emails that appear to come from managers, accountants, or other people who work for the organization.

Burt didn’t give the name or affiliation of the hackers other than to say they were sophisticated and had carried out the December campaign.

Beware of OAuth

It’s not the first time attackers have tricked targets into granting network access to malicious apps. Last year, researchers disclosed at least two others, both of them designed to gain access to Google accounts. One was carried out by hackers working for Egypt, according to a report from Amnesty International. The other targeted the iOS and Android devices of Tibetans.

Both campaigns relied on OAuth, an open standard that allows users to give websites or apps access to network resources without having to give them a password. As Microsoft said, such attacks often fly under the radar of users trained to spot phishing, since there’s no request to enter a password into a fake site. In some cases, the OAuth technique may have the ability to bypass two-factor authentication, which in addition to a password, requires users to enter a temporary password or to connect a physical security key to the device that’s being authenticated.

Microsoft’s Burt didn’t explicitly say the apps used in the more recent case connected through OAuth. In a separate post published on Wednesday, however, Microsoft warned of “Consent phishing,” in which attackers use the same OAuth method.

Among the advice the Microsoft posts provide to prevent such attacks is to turn on two-factor authentication. It’s always a good idea to turn on , but it’s not clear how effective the measure alone is at preventing these attacks. Some networks may not require the second factor for OAuth. And even when networks do enforce 2FA for OAuth, targets who are tricked into connecting an app can likely be fooled into supplying the second factor as well.

One way to protect Google and G Suite accounts against OAuth scams is to turn on Advanced Protection, which strictly enforces hardware-based 2FA for every new device or app

logging in for the first time. The program also restricts all but a handful of apps from connecting even when a key is provided, so it may not be suitable for all users. It’s possible that other 2FA protections do the same.

Other ways to avoid the scams is to learn the telltale signs of phishing, such as misspelled words, bad grammar, and links to sites that name a company or product but combine it with words that aren’t commonly used by the app maker or website operator. Wednesday’s post provides a variety of ways to spot malicious OAuth apps. These measures are hardly perfect, and as a result, the effectiveness and low cost of phishing makes it one of attackers’ go-to methods for compromising accounts. The steps are nonetheless worth following.

https://arstechnica.com/?p=1690316

Amid oil- and gas-pipeline halts, Dakota Access operator ignores court

Words projected onto the EPA’s headquarters during a demonstration.

reader comments

151 with 61 posters participating

Share this story

A series of decisions in the last few days has halted or scuttled three high-profile oil- and gas-pipeline projects. The Keystone and Dakota Access oil pipelines—sources of long-running controversy—both suffered legal setbacks that will require additional environmental impact reviews. Separately, the Atlantic Coast natural gas pipeline recently won a case before the US Supreme Court, yet it has now been abandoned by the two energy companies behind it.

The Keystone XL pipeline is meant to carry oil produced in Alberta, Canada, southeast to Nebraska, but it has suffered major delays. The Dakota Access pipeline, on the other hand, has been operational for several years, carrying oil from North Dakota to southern Illinois.

Both were subjected to major protests. The Keystone protests focused on the climate impact of facilitating production in Alberta's oil sands, where extraction is unusually energy intensive. Dakota Access was strongly opposed by the Standing Rock Sioux Tribe (and others), who feared the consequences of a leak where the pipeline crosses under the Missouri River on the edge of reservation land.

The Obama administration eventually denied approval to Keystone and halted work on Dakota Access while the Army Corps of Engineers reevaluated the proposed route. But immediately after taking office, President Trump pushed both projects forward, fast-tracking some remaining permits.

Those moves have been challenged in court, where tribal and environmental groups have argued that environmental review requirements were not being met. That argument has won out in recent decisions. A US District Court judge ruled in April that the Army Corps of Engineers should not have exempted the Dakota Access pipeline from completing an environmental impact analysis for the river crossing. On Monday, that same judge

ruled that the pipeline has to stop operating until the analysis is complete, giving a 30-day deadline to shut it down.

According to a Bloomberg report, however, Energy Transfer (the owner of the pipeline) is refusing that order. Instead, it's going right ahead with scheduling oil transport with its customers for August.

The Keystone pipeline also ran into District Court trouble back in April, when a judge decided that a long-standing Army Corps program allowing pipelines and other utility lines to skip many permitting requirements for river crossings is not legal. That lawsuit was focused on Keystone, but the ruling affected projects around the country.

Appealing

The decision is being appealed, but the Trump administration wanted the US Supreme Court to step in with an emergency ruling to prevent the change from taking effect until that process plays out. On Monday, the Supreme Court left the ruling in place for Keystone, preventing construction work from beginning. But the court did restore the current rules for any other projects.

This case was one of the factors cited by Dominion Energy and Duke Energy Sunday when they announced they had decided to drop the Atlantic Coast pipeline project, which was intended to carry natural gas through West Virginia, Virginia, and North Carolina. They argued that a stay from the Supreme Court "would not ultimately change the judicial venue for appeal nor decrease the uncertainty associated with an eventual ruling."

It is a surprising decision given that the companies won a Supreme Court case just last month about whether the pipeline could cross the Appalachian Trail. Some environmental groups had sued, arguing that the US Forest Service shouldn't have

granted the permit as the pipeline should not be allowed on National Park land. Obviously, it would be logistically difficult to ever run a pipeline on the East Coast without crossing the nearly 2,200-mile-long trail, and a number of pipelines already do. The Supreme Court decided that the Atlantic Coast pipeline's permit should stand.

Still, Duke and Dominion said that "ongoing delays and increasing cost uncertainty which threaten the economic viability of the project" pushed the companies to cancel it. Instead, Dominion decided to sell all of its natural gas pipeline and storage assets to "an affiliate" of prominent investor Warren Buffett's Berkshire Hathaway Inc.—a deal valued at $9.7 billion.

The Keystone and Dakota Access projects could ultimately win on appeal or resume after completing new environmental reviews. However, it's also possible that the government's position could change after the 2020 general election. But at least in the short-term, these court decisions have once again brought both pipelines to a halt.

https://arstechnica.com/?p=1690034

Harvard, MIT sue Trump admin to block deportation of online-only students

reader comments

181 with 107 posters participating

Share this story

Harvard University and the Massachusetts Institute of Technology today sued the Trump administration to block an action that forces foreign students with nonimmigrant visas to leave the United States or transfer to different schools that offer in-person classes. The schools' complaint, filed in US District Court for the District of Massachusetts, asks for a temporary restraining order and permanent injunction preventing the administration from enforcing the new policy issued by US Immigration and Customs Enforcement (ICE).

In the complaint, Harvard and MIT said:

> *By all appearances, ICE's decision reflects an effort by the federal government to force universities to reopen in-person classes, which would require housing students in densely packed residential halls, notwithstanding the universities' judgment that it is neither safe nor educationally advisable to do so, and to force such a reopening when neither the students nor the universities have sufficient time to react to or address the additional risks to the health and safety of their communities. The effect—and perhaps even the goal—is to create as much chaos for universities and international students as possible.*

The ICE policy will be especially problematic for Harvard and MIT students from certain countries, such as "Syria, where civil war and an ongoing humanitarian crisis make Internet access and study all but impossible," the lawsuit said. "Others come from Ethiopia, where the government has a practice of suspending all Internet access for extended periods, including presently, starting on June 30, 2020."

The policy also bars F-1 students who are currently outside the US "from entering or reentering the United States," the lawsuit said.

Online-only students may face "removal"

The ICE change to the Student and Exchange Visitor Program, announced Monday, said that "Nonimmigrant F-1 and M-1 students attending schools operating entirely online may *not* take a full online course load and remain in the United States." The US will not issue new visas to such students, and "[a]ctive students currently in the United States enrolled in such programs must depart the country or take other measures, such as transferring to a school with in-person instruction to remain in lawful status," ICE said. "If not, they may face immigration consequences including, but not limited to, the initiation of removal proceedings."

While a fully online course load isn't allowed, ICE said that nonimmigrant F-1 students may avoid deportation proceedings by attending schools that use a "hybrid model" of online and in-person classes.

This is a problem for thousands of students at Harvard and MIT. Harvard told students that "all course instruction (undergraduate and graduate) for the 2020-21 academic year will be delivered online," while MIT said that "most undergraduate instruction will take place online this fall," with lab work and some other types of instruction taking place "in small groups, when possible." Harvard has nearly 5,000 students who study in the US on F-1 visas, and MIT has nearly 4,000 such students.

Under the ICE rule change, F-1 students enrolled in an online-only program "must abandon housing arrangements they have made, breach leases, pay exorbitant air fares, and risk

COVID-19 infection on transoceanic flights" or "risk detention by immigration authorities and formal removal from the country" if they do not leave the US promptly, the schools' lawsuit said.

ICE didn't seek public comment, schools say

The Harvard/MIT suit points out that, on March 13, ICE issued an exemption to the rule that F-1 students must attend classes in person, at which time "the government made clear that this arrangement was 'in effect for the duration of the emergency.'" Yet the pandemic is raging on, and President Trump's "national emergency declaration has not been rescinded or terminated," the complaint said.

Harvard and MIT argue that ICE's ruling violates the US Administrative Procedure Act. The rule change "is arbitrary and capricious because it fails to consider important aspects of the problem before the agency… fails to offer any reasoned basis that could justify the policy," and it violates a requirement to provide public notice and take comments, the schools' lawsuit said.

Harvard and MIT told the court:

> *ICE's action proceeded without any indication of having considered the health of students, faculty, university staff, or communities; the reliance of both students and universities on ICE's statements that the preexisting exemptions would be "in effect for the duration of the emergency" posed by the COVID-19 pandemic, which continues to this day; or the absence of other options for universities to provide their curricula to many of their international students. Certainly, no notice-and-comment period was provided.*

> *ICE's action leaves hundreds of thousands of international students with no educational options within the United States. Just weeks from the start of the fall semester, these students are largely unable to transfer to universities providing on-campus instruction, notwithstanding ICE's suggestion that they might do so to avoid removal from the country. Moreover, for many students, returning to their home countries to participate in online instruction is impossible, impracticable, prohibitively expensive, and/or dangerous.*

The ICE action gives schools "an impossible choice: lose numerous students who bring immense benefits to the school or take steps to retain those students through in-person classes, even when those steps contradict each school's judgment about how best to protect the health of the students, faculty, staff, and the entire university community," the complaint also said.

Princeton University announced that it is filing a brief supporting the Harvard/MIT lawsuit.

"ICE is unable to offer the most basic answers"

ICE argues in an FAQ that its new approach "carefully balance[s] public health concerns against the varied approaches that schools and universities are taking to combat the spread of COVID-19." ICE also said that "the health and safety of all students is of the utmost importance" but said government officials determined that "remote learning from outside the United States, in-person classes, and a hybrid model that combined both in-person and online classes provided the best options for flexibility for nonimmigrant students to continue education with health risks associated with international travel at this time."

The ICE FAQ said the Department of Homeland Security "coordinated with its government partners" at the State Department and US Customs and Border Protection before making the change. But Harvard and MIT say the concerns of schools and students were ignored.

"The announcement disrupts our international students' lives and jeopardizes their academic and research pursuits," MIT President L. Rafael Reif wrote, adding that "ICE is unable to offer the most basic answers about how its policy will be interpreted or implemented."

Meanwhile, President Trump today criticized the Centers for Disease Control and Prevention for issuing what he called "very tough & expensive guidelines for opening schools" and threatened to "cut off funding" if schools don't reopen this fall.

https://arstechnica.com/?p=1690227

Hong Kong downloads of Signal surge as residents fear crackdown

d3sign / Getty

reader comments

94 with 60 posters participating

Share this story

The secure chat app Signal has become the most downloaded app in Hong Kong on both Apple's and Google's app stores, Bloomberg reports, citing data from App Annie. The surging interest in encrypted messaging comes days after the Chinese government in Beijing passed a new national security law that reduced Hong Kong's autonomy and could undermine its traditionally strong protections for civil liberties.

The 1997 handover of Hong Kong from the United Kingdom to China came with a promise that China would respect Hong Kong's autonomy for 50 years following the handover. Under the terms of that deal, Hong Kong residents should have continued to enjoy greater freedom than people on the mainland until 2047. But recently, the mainland government has appeared to renege on that deal.

Civil liberties advocates see the national security law approved last week as a major blow to freedom in Hong Kong. The New York Times reports that "the four major offenses in the law—separatism, subversion, terrorism and collusion with foreign countries—are ambiguously worded and give the authorities extensive power to target activists who criticize the party, activists say." Until now, Hong Kongers faced trial in the city's separate, independent judiciary. The new law opens the door for dissidents to be tried in mainland courts with less respect for civil liberties or due process.

This has driven heightened interest among Hong Kongers in secure communication technologies. Signal offers end-to-end encryption and is viewed by security experts as the gold standard for secure mobile messaging. It has been endorsed by NSA whistleblower Ed Snowden.

One of Signal's selling points is that it minimizes data collection on its users. When rival Telegram announced it would no longer honor data requests from Hong Kong courts,

Signal responded that it didn’t have any user data to hand over in the first place.

Bloomberg has also reported on the surging adoption of VPN software in Hong Kong as residents fear government surveillance of their Web browsing.

https://arstechnica.com/?p=1690144

Trump administration “looking into” ban on TikTok, other Chinese apps

Enlarge / A stand of TikTok (Douyin) at The First International Artificial Products Expo Hangzhou on October 18, 2019, in Hangzhou, China.

reader comments

128 with 91 posters participating

Share this story

Trade War! USA v. China

View more stories

The Trump administration is considering banning Chinese social media apps inside the United States, Secretary of State Mike

Pompeo said Monday. The ban would start with popular short-video platform TikTok.

“We’re taking this very seriously. We’re certainly looking at [TikTok],” Pompeo said during a televised interview with Fox News. He directly and explicitly linked the considered ban on TikTok and other apps to the administration’s actions against other Chinese tech firms.

“We’ve worked on this very issue for a long time, whether it was the problems of having Huawei technology in your infrastructure, we’ve gone all over the world and we’re making real progress getting that out,” he said. “We declared ZTE a danger to American national security, we’ve done all of these things. With respect to the Chinese apps on people’s cell phones I can assure you the United States will get this one right. I don’t want to get out in front of the president, but it’s something we’re looking at.”

Pompeo concluded by recommending users download TikTok “only if you want your private information in the hands of the Chinese Communist party.”

“TikTok is led by an American CEO, with hundreds of employees and key leaders across safety, security, product, and public policy here in the US,” the company said in response to Pompeo’s statement. “We have no higher priority than promoting a safe and secure app experience for our users. We have never provided user data to the Chinese government, nor would we do so if asked.”

A national security risk?

Pompeo’s interview was not the first time US officials have expressed concern over TikTok’s data-collection practices—and the questions have not been limited to the White House or to a single party.

Senators Tom Cotton (R-Ark.) and Chuck Schumer (D-N.Y.) last October asked the Director of National Intelligence to launch a probe into TikTok and its parent company ByteDance. “TikTok’s terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information,” the senators wrote at the time. “While the company has stated that TikTok does not operate in China and stores US user data in the US, ByteDance is still required to adhere to the laws of China.”

A week later, reports surfaced that the Committee on Foreign Investment in the United States (CFIUS) was indeed investigating the companies on national security grounds. CFIUS, headed by the Treasury Department, brings together members from a dozen different agencies that conduct national security reviews when an international business acquires a US business. CFIUS had its scope and mandate greatly expanded in 2018 when President Trump signed a “modernization” package into law.

TikTok in the US started life in 2014 as the startup, short-form video app Musical.ly. A division of Beijing-based ByteDance—TikTok—snapped up Musical.ly for close to $1 billion in late 2017. In 2018, it decided to sunset the Musical.ly name and product, integrating the two extremely similar apps under the TikTok name. CFIUS did not review the Musical.ly acquisition in 2017, so the committee had authority to launch the investigation retroactively.

Reuters in May was first to report that ByteDance has been actively transferring TikTok’s operations out of China by hugely expanding its presence in California. “The strategy is aimed not only at TikTok, which is not available in China, but all of ByteDance’s non-China focused businesses,” Reuters wrote. Reuters included India-based social networking app Helo in its non-China businesses.

Where India is concerned, that move came too late. TikTok and almost 60 other Chinese apps were banned in India last week after a fatal military confrontation between the India and China border earlier in June. Indian officials said the apps were “stealing and surreptitiously transmitting users’ data in an unauthorized manner to servers which have locations outside India.” Those officials added, “The compilation of these data, its mining and profiling by elements hostile to national security and defense of India, which ultimately impinges upon the sovereignty and integrity of India, is a matter of very deep and immediate concern which requires emergency measures.”

Privacy problems

Whether or not Chinese political entities are accessing TikTok user data, its privacy practices more generally are also now the subject of widespread concern.

In May, a group of 20 children’s, consumer, and privacy advocacy groups filed a complaint with the Federal Trade Commission over TikTok’s handling of children’s personal data. The groups claimed TikTok was violating a 2019 settlement the FTC reached with TikTok predecessor Musical.ly over alleged violations of the Children’s Online Privacy Protection Act (COPPA). The company paid $5.7 million, at the time the largest civil penalty ever imposed by the FTC in a COPPA case, to settle claims that it knowingly harvested and used personal data from users under age 13 without obtaining parental consent.

In June, researchers found that TikTok was collecting clipboard data from iOS users. All kinds of sensitive information, including account passwords, often reside on a device’s clipboard after users copy it from one field to paste it somewhere else.

The flaw was first discovered in March. At that time, TikTok promised to end the practice “in the next few weeks.” But

clearly it has not.

https://arstechnica.com/?p=1689839

Trump “officially” takes US out of WHO, but withdrawal is a year-long process

reader comments

182 with 105 posters participating

Share this story

The Trump administration has officially withdrawn the United States from the World Health Organization, according to a Democratic senator and multiple news reports. But the withdrawal process will take a year, so Trump may not be able to see it through.

“Congress received notification that POTUS officially withdrew the US from the WHO in the midst of a pandemic,” Sen. Bob Menendez (D-N.J.) wrote on Twitter today. “To call Trump’s response to COVID chaotic and incoherent doesn’t do it justice. This won’t protect American lives or interests—it leaves Americans sick and America alone.”

According to The Hill, a senior Trump administration official confirmed today that “the White House has officially moved to

withdraw the United States from the World Health Organization."

"The US has submitted its withdrawal notification to the United Nations secretary-general, the official said," according to The Hill article. "Withdrawal requires a year's notice, so it will not go into effect until July 6, 2021, raising the possibility the decision could be reversed." That would be six months after the next presidential inauguration.

"The notice to the UN was the first step in a yearlong process that will rely on several factors outside of Trump's control, including cooperation from Congress and Trump's own reelection in November, neither of which are assured," CNBC wrote. The Washington Post also confirmed that the Trump administration sent a letter to the United Nations withdrawing the US from the WHO "over its handling of the coronavirus pandemic."

A WHO spokesperson told Ars, "We have received reports that the US has submitted formal notification to the UN Secretary General that it is withdrawing from WHO effective 6 July 2021. We have no further information on this at this stage."

1948 joint resolution requires year-long process

The question of whether Trump can unilaterally take the United States out of the WHO is addressed in a recent Congressional Research Service report. It says that the 1948 joint resolution by Congress authorizing the president to accept membership in the WHO puts limits on Trump's authority here:

> *This resolution reserved the right of the "United States" to withdraw from the organization after a one-year notice, and specified that US financial obligations to the organization must be met in full for the organization's "current fiscal year" before withdrawal could become effective. The*

> *resolution does not specify whether the "United States" includes the President as Head of State acting alone to effect withdrawal or the President and Congress acting jointly to accomplish withdrawal (e.g., by joint resolution). However, even if the 1948 joint resolution contemplates the President acting alone, the joint resolution appears to impose two conditions on the President's withdrawal from the organization: (1) that the President provide a one-year notice; and (2) that the United States meet its financial obligations to the organization in full for the organization's current fiscal year before withdrawing.*

Because of this, "it appears that the joint resolution would only prohibit the President from withdrawing *immediately*. The President could, consistent with the joint resolution, submit a notice of intent to withdraw, but it would not take effect for at least twelve months." A court may ultimately have to rule on the matter, the report said.

The WHO apparently lacks authority to mandate payment, but it "may suspend US voting rights if, during the twelve-month notice period, it finds the United States to be in arrears," the report said. Congress can also "consider imposing additional conditions on withdrawal," the report said.

Trump had been threatening to take the US out of the WHO for months. In April, he halted US funding to the United Nations health agency, then announced in May that the US government is "terminating our relationship" with the WHO.

"China has total control over the World Health Organization despite only paying $40 million per year, compared to what the United States has been paying, which is approximately $450 million a year," Trump said at the time, while blaming the WHO for not being tough enough on China during the COVID-19 pandemic. Trump hadn't followed through on the plan to withdraw from the WHO as of mid-June, but he has now taken

action—albeit an action that could be reversed, particularly if he loses his bid for reelection.

https://arstechnica.com/?p=1689929

Does First Amendment let ISPs sell Web-browsing data? Judge is skeptical

reader comments

62 with 46 posters participating

Share this story

The broadband industry has lost a key initial ruling in its bid to kill a privacy law imposed by the state of Maine.

The top lobby groups representing cable companies, mobile carriers, and telecoms sued Maine in February, claiming the privacy law violates their First Amendment protections on free speech and that the state law is preempted by deregulatory actions taken by Congress and the Federal Communications Commission. Maine's Web-browsing privacy law is similar to the one killed by Congress and President Donald Trump in 2017, as it prohibits ISPs from using, disclosing, or selling browsing history and other personal information without customers' opt-in consent. The law took effect on July 1, 2020.

The case is not over, but the ruling today by Judge Lance Walker in US District Court for the District of Maine dealt a major blow to the broadband industry's lawsuit. The plaintiffs representing the broadband industry are America's Communications Association, CTIA, NCTA, and USTelecom. Walker denied the plaintiffs' motion for judgment on the pleadings, criticized the industry's First Amendment argument, and granted Maine's motion to dismiss claims that the state law is preempted by federal law.

The judge agreed with the broadband industry that "plaintiffs' marketing of customer data… is sheltered by the First Amendment," but he added that "not all speech deserves the same level of protection." Commercial speech "is ordinarily accorded less First Amendment protection than are other forms of constitutionally guaranteed expression," he noted. The judge agreed with the Pine Tree State that its privacy law should be "subject to intermediate scrutiny" under a First Amendment analysis, instead of the "strict scrutiny" standard proposed by the broadband industry.

The judge also found that "Plaintiffs' Motion simply fails to clarify how an ill-defined opt-in and opt-out regime would inhibit any protected First Amendment activity; for example, how it might chill them from preparing particular marketing materials for sale to customers. And, they have not begun to bear their burden to show the statute would be unconstitutional in 'all of its applications,' as they must for a facial challenge." These findings will make it harder for ISPs to prove Maine's law violates the First Amendment.

"While Judge Walker allowed the broadband industry's argument that the Maine law violates the First Amendment to proceed, he ruled that the law is not unconstitutional on its face and clearly expressed skepticism that the industry would succeed at trial," Gigi Sohn, a consumer advocate and former Obama-era FCC official, said today. "Judge Walker refused to apply a strict scrutiny standard to the law, instead applying an

intermediate First Amendment scrutiny that applies to commercial speech. He also firmly rejected broadband providers' overwrought allegations of harm."

Judge calls FCC preemption "dubious"

The judge ruled against ISPs' claims that the Maine law is preempted by actions taken by Congress and the FCC. Contrary to the industry's claim, the judge found that Congress's decision to eliminate Obama-era FCC privacy rules "creates no overarching federal policy, and enacts no scheme with which the Maine Privacy Statute can conflict."

The judge also said Maine's law does not conflict with the Trump-era FCC's decision to deregulate the broadband industry as part of its net neutrality repeal. Walker wrote:

> *Not only is the FCC's abdication of authority in favor of the FTC of dubious preemptive effect, but Plaintiffs also have failed to identify any conflict between the FCC's proclamation that the FTC [Federal Trade Commission] is the proper federal regulator of ISPs [in the net neutrality repeal order] and Maine's decision to impose privacy protections at the state level. The idea that the FCC's relinquishment of authority over ISPs creates a federal scheme prohibiting state privacy regulation of ISPs blinks reality.*

Walker granted Maine's motion for judgment against the industry's claims that the Maine law conflicts with the congressional and FCC orders. The judge also denied an industry motion "to invalidate the Privacy Statute as unconstitutionally vague due to its geographic scope."

FCC Chairman Ajit Pai tried to wipe out all current and future state net neutrality rules in his net neutrality repeal order,

but Walker isn’t the first judge to find that the FCC repeal doesn’t automatically invalidate state laws. The US Court of Appeals for the District of Columbia Circuit last year upheld the repeal itself, but it simultaneously vacated the FCC’s attempt at a blanket, nationwide preemption.

“ISPs welcomed the Pai FCC’s decision to abdicate authority over broadband with open arms,” said Legal Director John Bergmayer of consumer-advocacy group Public Knowledge. “This opened the door to states regulating broadband practices, as Maine has done. The argument that somehow states lack this authority was rejected by the DC Circuit in the Mozilla [vs. FCC] case, and here as well. This bodes well for other state efforts to protect the privacy of broadband users and open Internet principles.”

Sohn said that if ISPs “prevail at trial and beyond, the future of national and state privacy laws will be at risk, as will nearly any attempt to protect consumers and competition in the broadband market.” But she called today’s ruling “a good first step towards deflating the providers’ ‘shoot-the-moon’ attempt to use the First Amendment as a deregulatory tool.”

https://arstechnica.com/?p=1689885

City builds open-access broadband network with Google Fiber as its first ISP

Enlarge / Illustration of fiber-optic cables.
Getty Images | Tetra Images

reader comments

90 with 54 posters participating, including story author

Share this story

Google Fiber’s wireline broadband is expanding to a new city for the first time in several years as part of a public-private partnership to build an open-access network that any ISP can use to offer service. The new network will be in West Des Moines, Iowa.

Google Fiber “paused” plans to expand to new cities in October 2016 amid lawsuits filed by incumbent ISPs and construction problems that eventually led to the Alphabet-owned ISP’s complete exit from Louisville. But in West Des Moines, Google Fiber will rely on the city to build a network of fiber conduits.

“Municipalities like West Des Moines excel at building and maintaining infrastructure. At digging and laying pipes under the roads, restoring and preserving the sidewalks and green spaces, reducing traffic congestion, and lowering construction disruption,” Google Fiber said in an announcement yesterday.

The West Des Moines government’s announcement said that “once the City installs conduit in the public right of way, broadband providers will pay a license fee to install their fiber in the City’s conduit. Google Fiber will be the first tenant in the network.” A conduit-license agreement “calls for Google Fiber to cover a portion of the construction cost to build conduit… through their monthly lease payments.”

“On a monthly basis, Google Fiber would pay the city $2.25 for

each household that connects to the network," according to the Des Moines Register. Google Fiber would pay the city a minimum of $4.5 million over 20 years.

Construction is expected to begin this fall and be completed in about two and a half years, the city said. While Google Fiber is slated to be the first tenant offering fiber service over the West Des Moines network, the city is hoping to spur broadband competition by letting other ISPs install their own fiber in the conduits.

Current ISPs in West Des Moines include CenturyLink and Mediacom.

City aims to cover all homes and businesses

Google Fiber's previous buildouts have only covered a portion of each city, based on where demand was highest. But West Des Moines is aiming for universal coverage, and Google Fiber said it will offer service "city-wide."

"Every home and business in West Des Moines is eligible for a free connection point from their property to the municipal fiber conduit," the city said. "The City will be installing these connections and will contact every business and resident in the near future to ensure everyone has the opportunity to participate." The city also said it aims to make high-speed broadband available to "all residents, regardless of their means."

The city said it will pay for its portion of the building costs by issuing bonds instead of raising property taxes. "West Des Moines plans to invest nearly $40 million" in the project, the Des Moines Register wrote, adding that city officials intend to "solicit bids for laying the underground conduit that would house the fiber-optic cables."

While Google Fiber largely gave up on its own fiber construction, it offers wireless home-Internet service in some cities through its Webpass subsidiary. Google Fiber's announcement said the ISP will continue to "explore partnerships" with other cities:

> *This isn't the first time Google Fiber has collaborated with a city to create a fiber optic network. In Huntsville, Alabama, we lease fiber from Huntsville Utilities to provide high speed internet service across that city.*
>
> *Whether in Huntsville, in West Des Moines, or anywhere else, our goal is to work with communities to find the right model that brings world-class Internet to more people and businesses, and that increases competition. We will continue to explore partnerships with other forward-thinking cities, utilities, and enterprises. After all, there is still so much more to do to make internet service faster and more affordable and enable everyone to get the great Internet they deserve.*

The list of cities where Google Fiber offers either wireline or wireless service is available here. Google Fiber reached out to Ars after this article published to note that "we're continuing to build out our networks in all of our existing Google Fiber cities. In West Des Moines, however, we're using a new model that allows the city and Google Fiber to focus on what we do best."

https://arstechnica.com/?p=1689808