Senator wants to know if police are using Clearview to ID protesters

Enlarge / Police using facial recognition software could possibly identify thousands of Americans nationwide as participants in protests against police brutality and overreach. Including this group in Minneapolis, Minnesota, on June 5.

reader comments

34 with 21 posters participating

Share this story

Secretive facial-recognition firm Clearview AI is facing new questions from lawmakers, in addition to lawsuits, as concerns about its software are amplified during the wave of nationwide protests against police brutality.

Sen. Edward Markey (D-Mass.) today demanded to know what law enforcement agencies are working with Clearview potentially to identify protesters who are out in support of black communities and against police violence. “As demonstrators across the country exercise their First Amendment rights by protesting racial injustice, it is important that law enforcement does not use technological tools to stifle free speech or endanger the public,” Markey wrote in a letter to Clearview (PDF). “The risk of such omnipresent surveillance also runs the risk of deterring Americans from speaking out.”

Law enforcement agencies in several cities where protests have taken place are using digital surveillance tools. According to

a BuzzFeed report, many law enforcement agencies in and near Minneapolis—where current national protests began after police were recorded killing George Floyd—use Clearview and other similar platforms to identify individuals.

Clearview operated largely without the public knowing about it until January, when The New York Times published a detailed report about the company. The Times described Clearview as a "groundbreaking" facial-recognition service, which allowed a user to match an imported photo against a database of more than 3 billion images.

Those facial images against which Clearview matches imported photos were scraped from basically the entire rest of the Internet, including Facebook, Google, YouTube, LinkedIn, and others. Once the report drew public attention to this, those companies' legal teams all sent Clearview demands to stop at once.

The company claimed to have about 600 law enforcement customers at the time of the NYT report, but it has repeatedly refused to make public its client list, including in response to previous requests from Markey's office. However, after obtaining a leaked client list from a data breach, BuzzFeed in February reported more than 2,200 agencies, businesses, and individuals had performed searches on Clearview's platform.

In addition to requesting a client list again, Markey's newest letter explicitly asks Clearview if it will prohibit its customers from using its technology "to monitor or identify peaceful protesters" and if it will expand the mechanism Illinois and California residents can use to have their images removed to residents of all 50 states—and if not, why not?

Illinois law does regulate the collection and use of individuals' biometric information, and late last month the American Civil Liberties Union filed a lawsuit against Clearview in Illinois alleging violations of that law.

“Clearview’s business model appears to embody the nightmare scenario… a private company capturing untold quantities of biometric data for purposes of surveillance and tracking without notice to the individuals affected, much less their consent.”

The ACLU suit is not the first Clearview is facing. Vermont Attorney General T.J. Donovan also filed suit against Clearview in March, alleging multiple violations of state law regulating data-broker behavior.

https://arstechnica.com/?p=1681942

Tear gas is more dangerous than police let on—especially during the pandemic

Enlarge / A woman holds a placard reading ‘I can’t breathe’ amid tear gas in Toulouse, France.
Alain Pitton/NurPhoto via Getty Images

reader comments

372 with 111 posters participating

Share this story

When Amira Chowdhury joined a protest in Philadelphia against police violence on Monday, she wore a mask to protect herself and others against the coronavirus. But when officers launched

tear gas into the crowd, Chowdhury pulled off her mask as she gasped for air. “I couldn’t breathe,” she said. “I felt like I was choking to death.”

Chowdhury was on a part of the Vine Street Expressway that ran underground. Everyone panicked as gas drifted into the dark, semi-enclosed space, she said. People stomped over her as they scrambled away. Bruised, she scaled a fence to escape. But the tear gas found her later that evening, inside her own house; as police unleashed it on protesters in her predominantly black neighborhood in West Philadelphia, it seeped in.

“I can’t even be in my own house without escaping the violence of the state,” said Chowdhury, a rising senior at the University of Pennsylvania. On Wednesday, she said her throat still felt dry, like it was clogged with ash.

The Philadelphia protest was one of many instances in recent days in which police launched tear gas — a toxic substance that can cause lung damage — into crowds. In a statement, Police Commissioner Danielle Outlaw said that officers had no choice but to release it after protesters threw rocks at them and refused to disperse and that officers also used nonchemical white smoke to minimize the amount of the irritant “while maintaining a deterrent visual effect.” She called it “a means to safely [defuse] a volatile and dangerous situation.”

But tear gas is not safe, according to a number of experts interviewed by ProPublica. It has been found to cause long-term health consequences and can hurt those who aren’t the intended targets, including people inside their homes.

This would be enough of a problem in normal times, but now, experts say, the widespread, sometimes indiscriminate use of tear gas on American civilians in the midst of a respiratory pandemic threatens to worsen the coronavirus, along with racial disparities in its spread and who dies from it.

“As an immunologist, it scares me,” said Dr. Purvi Parikh, an allergy and immunology doctor at NYU Langone Health. “We just got through a brutal two months, and I’m really scared this will bring a second wave [of COVID-19] sooner.”

It puts black communities in an impossible situation, said Dr. Joseph Nwadiuko, an internist and researcher at the University of Pennsylvania Perelman School of Medicine. Thirteen of the 15 coronavirus patients in the intensive care unit where he works are black, he said. “I worry that one of the compounding effects of structural racism is you’ll see a second wave of black patients, including those who were out there defending their lives.”

On Tuesday, an open letter signed by nearly 1,300 medical and public health professionals urged the police to stop using “tear gas, smoke, or other respiratory irritants, which could increase risk for COVID-19 by making the respiratory tract more susceptible to infection, exacerbating existing inflammation, and inducing coughing.”

Here’s what you need to know about tear gas and how it’s being used by law enforcement in recent days.

Tear gas can cause long-term harm by making people more susceptible to contracting influenza, pneumonia, and other illnesses

Tear gas is the generic term for a class of compounds that cause a burning sensation. Most law enforcement agencies in the US, including the Philadelphia Police Department this week, use a chemical called CS, short for 2-chlorobenzalmalononitrile.

CS activates a specific pain receptor, one that’s also

triggered by eating wasabi, said Sven-Eric Jordt, a professor of anesthesiology at Duke University. But CS is much more powerful, up to 100,000 times stronger than the sting from wasabi, he said.

“They are really pain nerve gases. They are designed to induce pain.”

CS is particularly painful when it gets on your skin or in your eyes. (Doctors have advised protesters not to wear contact lenses.) When inhaled, the pain induces people to cough. The compound degrades the mucus membranes in your eyes, nose, mouth and lungs—the layers of cells that help protect people from viruses and bacteria.

Scientists know little about how CS affects the general public. The most comprehensive studies were conducted by the US military on thousands of recruits who were exposed to tear gas during training exercises. Afterward, it left them at higher risk for contracting influenza, pneumonia, bronchitis and other respiratory illnesses.

The soldiers were generally healthier than the average person, with fewer underlying conditions like asthma or heart disease. Studies of civilians in Turkey found that people who are repeatedly exposed to tear gas are more likely to have chronic bronchitis or chest pains and coughing that can last for weeks. It may also be linked to miscarriages.

The effects worsen as people are repeatedly exposed to higher doses, Jordt said, but it’s hard to measure the concentrations of tear gas during chaotic protests, and many who are affected will be reluctant or afraid to seek medical help.

Parikh, the Langone Health doctor, is particularly worried about children at the protests. Their lungs and immune system are still developing, and tear gas could lead to neurological problems or permanent skin or eye damage if it’s not washed off quickly.

According to the Centers for Disease Control and Prevention, severe tear gas poisoning, particularly if the gas was released in an enclosed space — can blind or kill people through chemical burns and respiratory failure. Prisoners with respiratory conditions have died after inhaling tear gas in poorly ventilated areas. On Wednesday, an inmate at the Metropolitan Detention Center in Brooklyn died after guards sprayed him with pepper spray, another kind of tear gas that causes similar health effects as CS.

In a statement, the US Department of Justice's Bureau of Prisons said the inmate, Jamel Floyd, was caught "breaking the cell door window with a metal object" and "became increasingly disruptive and potentially harmful to himself and others." Medical staff "immediately responded to assess the inmate, found Mr. Floyd to be unresponsive, and instantly initiated life-saving measures." An investigation is underway.

https://arstechnica.com/?p=1681620

Iran- and China-backed phishers try to hook the Trump and Biden campaigns

reader comments

40 with 31 posters participating

Share this story

State-backed hackers from Iran and China recently targeted the presidential campaigns of Republican President Donald Trump and Democrat Joe Biden, a Google threat analyst said on Thursday.

The revelation is the latest evidence of foreign governments attempting to gain intelligence on US politicians and potentially disrupt or meddle in their election campaigns. An Iran-backed group targeted the Trump campaign, and China-backed attackers targeted the Biden campaign, said Shane Huntley, the head of Google's Threat Analysis Group on Twitter. Both groups used phishing emails. There's no indication that either attack campaign succeeded.

Kittens and Pandas

Huntley identified the Iranian group that targeted Trump's campaign as APT35, short for Advanced Persistent Threat 35. Also known as Charming Kitten, iKittens, and Phosphorous, the group was caught targeting an unnamed presidential campaign before, Microsoft said last October. In that campaign, Phosphorous members attempted to access email accounts campaign staff received through Microsoft cloud services. Microsoft said that the attackers worked relentlessly to gather information that could be used to activate password resets and other account-recovery services Microsoft provides.

The Chinese group known as APT31, meanwhile, targeted the Biden campaign, Huntley said. The group, which security researchers also call Hurricane Panda, Black Vine, and Zirconium, "is a highly advanced adversary" that in 2014 exploited a zeroday vulnerability in Microsoft Windows, researchers from security firm CrowdStrike said at the time.

Google responds

Huntley said that Google officials sent the campaigns the company's standard warning that they were targeted by nation-based hacking. The company began the practice in 2012. To protect its sources and methods, Google doesn't send the notifications immediately and then dispatches them in large batches. Google also referred the matter to law enforcement.

In a statement, a Google spokesman wrote:

> *We can confirm that our Threat Analysis Group recently saw phishing attempts from a Chinese group targeting the personal email accounts of Biden campaign staff and an Iranian group targeting the personal email accounts of Trump campaign staff. We didn't see evidence that these attempts were successful. We sent the targeted users our standard government-backed attack warning and we referred this information to federal law enforcement. We encourage campaign staff to use extra protection for their work and personal emails, and we offer security resources such as our Advanced Protection Program and free security keys for qualifying campaigns.*

Hacking political parties and campaigns has been a chief concern ever since two Russian hacking groups were caught breaking into the network of the Democratic National Committee in 2016, just ahead of the presidential campaign. The breaches were largely achieved using phishing emails that tricked staff members into entering their passwords into attacker-controlled sites.

Multiple US intelligence agencies later concluded that Russia engaged in a sustained hacking and disinformation campaign with the goal of disrupting the US democratic process and to boost then-candidate Trump's chances of winning the election.

Google provides the above-mentioned Advanced Protection Program, a service that’s designed to protect politicians, election workers, journalists, and other people who are frequently targeted by hackers. The program requires a physical security key to be used as a second factor when logging in to Gmail and other Google services from new devices. APP would have very likely thwarted the 2016 phishing attacks since the mere stealing of passwords is insufficient to gain unauthorized access.

https://arstechnica.com/?p=1681486

Instagram just threw users of its embedding API under the bus

reader comments

46 with 37 posters participating, including story author

Share this story

Instagram does not provide users of its embedding API a copyright license to display embedded images on other websites, the company said in a Thursday email to Ars Technica. The announcement could come as an unwelcome surprise to users who believed that embedding images, rather than hosting them directly, provides insulation against copyright claims.

“While our terms allow us to grant a sub-license, we do not grant one for our embeds API,” a Facebook company spokesperson told Ars in a Thursday email. “Our platform policies require third parties to have the necessary rights from applicable rights holders. This includes ensuring they have a license to share this content, if a license is required by law.”

In plain English, before you embed someone’s Instagram post on your website, you may need to ask the poster for a separate license to the images in the post. If you don’t, you could be subject to a copyright lawsuit.

Professional photographers are likely to cheer the decision, since it will strengthen their hand in negotiations with publishers. But it could also significantly change the culture of the Web. Until now, people have generally felt free to embed Instagram posts on their own sites without worrying about copyright concerns. That might be about to change.

Two lawsuits, different results

Newsweek recently found this out the hard way. Photographer Elliot McGucken took a rare photo (perhaps this one) of an ephemeral lake in Death Valley. Ordinarily, Death Valley is bone dry, but occasionally a heavy rain will create a sizable body of water. Newsweek asked to license the image, but McGucken turned down their offer. So instead Newsweek embedded a post from McGucken’s Instagram feed containing the image.

McGucken sued for copyright infringement, arguing that he hadn’t given Newsweek permission to use the photo. Newsweek countered that it didn’t need McGucken’s permission because it could get rights indirectly via Instagram. Instagram’s terms of service require anyone uploading photos to provide a copyright license to Instagram—including the right to sublicense the same rights to other users. Newsweek argued that that license extends to users of Instagram’s embedding technology, like Newsweek.

Newsweek had reason to be optimistic about this argument because Mashable won a very similar case in April. The judge in the Mashable case ruled that photographer Stephanie Sinclair "granted Instagram the right to sublicense the photograph, and Instagram validly exercised that right by granting Mashable a sublicense to display the photograph."

But in a surprise ruling on Monday, Judge Katherine Failla refused to dismiss McGucken's lawsuit at a preliminary stage. She held that there wasn't enough evidence in the record to decide whether Instagram's terms of service provided a copyright license for embedded photos.

Instagram's bombshell

Now Instagram has dropped another bombshell that throws the entire premise of Newsweek's defense into doubt.

"Wow. That is going to blow up the *Sinclair* case," Cornell copyright scholar James Grimmelmann wrote after I shared Instagram's comment with him.

By stating outright that users of its embedding feature don't get licenses from Instagram to display photos, Instagram is preventing future defendants from using Mashable's argument. It will be hard for Newsweek to convince a judge that it had a sublicense from Instagram when Instagram has explicitly claimed the opposite.

Instagram tells Ars that it's exploring the possibility of giving users more control over photograph embedding. Right now, Instagram users can block embedding of their posts by switching their Instagram account to private. But that will also prevent users on the Instagram platform from seeing their content, too, which can be a career liability for professional photographers. Right now, Instagram offers no option to make content public inside the Instagram app while disabling embedding on external websites.

Kim Almazan, a copyright litigator at the law firm of Withersworldwide, argues that the safest route is for media companies to ask photographers for permission before embedding their work in news articles—and to use another photo if the photographer says no.

The “server test” is more important than ever

Newsweek has a couple of other legal options. Newsweek claimed fair use, but Judge Failla seemed skeptical of this argument in Monday’s ruling.

Grimmelmann pointed to another argument Newsweek might raise: that Instagram—not Newsweek—was the distributor of the photograph.

An embedded Instagram post is actually a bit of code that instructs the user’s browser to fetch the contents of a post—such as McGucken’s photograph—directly from Instagram’s servers. In the past, courts have ruled against plaintiffs in embedding cases based on the “server test,” which holds that liability goes to whomever runs the server that actually delivers infringing content to the user—in this case, Instagram.

This argument is binding law in the 9th Circuit, which includes California (and therefore covers a lot of technology companies). Appeals courts in most other circuits haven’t ruled on the question one way or the other. A federal trial judge in New York rejected the server test 2018, creating a worrying precedent for defendants. But because it was only a trial court ruling, it wasn’t binding on other judges.

Instagram’s decision to throw users of its embedding API under the bus makes the server test crucial for cases like this. If the server test is adopted outside the 9th Circuit, it could

provide a legal basis for the continued use of embedded Instagram posts. On the other hand, if the 2nd Circuit—which covers New York—ultimately rejects the server test, then it would become legally hazardous to use Instagram embeds without a separate copyright license.

Grimmelmann notes that Facebook's statement is "studiously noncommittal" about whether the server test is the law.

At this point, Newsweek's best chance is likely to be to raise a server test defense. Eventually, the case may make its way to the 2nd Circuit Appeals Court, which will have to decide whether it wants to follow 9th Circuit precedent—which could make it a *de facto* national standard—or reject the server test and throw the legality of embedding into doubt nationwide.

https://arstechnica.com/?p=1681121

The Pentagon's hand-me-downs helped militarize police. Here's how

Enlarge / A Miami Police officer watches protesters from an armored vehicle on May 31, 2020.
Richard Arduengo | Getty Images

reader comments

196 with 101 posters participating

Share this story

The images of this past week are both inescapable and indelible: protesters flooding the streets of cities across the United States, met by police forces equipped with full body armor and tactical vehicles that vaguely resemble tanks. The local law enforcement responding to even nonviolent protests has often looked more like the US Armed Forces—and that was before President Donald Trump deployed an actual military police battalion against peaceably assembled US citizens in the nation's capitol Monday. That's no accident.

It's easy enough to buy tactical gear in the US, and the Homeland Security Grant Program has funneled billions of dollars to law enforcement agencies to acquire military-grade equipment. But for decades, a primary driver for why it can be so hard to tell a National Guard troop from a local cop has been the Department of Defense itself, through a program that has parceled out everything from bayonets to grenade launchers to precincts across the country.

Created as part of 1997's National Defense Authorization Act, the 1033 program allows the Department of Defense to get rid of excess equipment by passing it off to local authorities, who only have to pay for the cost of shipping. (A precursor, the slightly more restrictive 1208 program, began in 1990.) According to the Law Enforcement Support Office (LESO), which oversees the process, over $7.4 billion of property has been transferred since the program's inception; more than 8,000 law enforcement agencies have enrolled. Much of that inventory is perfectly ordinary: office equipment, clothing, tools, radios, and so on. But the haul also includes some of the so-called controlled equipment—rifles, armored vehicles, and so on—that have helped create such a spectacle of disproportion.

Those displays are not unique to the current protests against

police brutality, either. The militarization of the American police, and the 1033 program specifically, began attracting wider scrutiny in 2014, after the Black Lives Matter protests in Ferguson, Missouri.

Proponents of the 1033 program say that it keeps cities safer. Detractors say the distribution of controlled items actually increases police violence. Widely circulated studies have argued both sides. But those who have examined the 1033 program in depth more recently argue that the real problem is that no one knows for sure either way, because years of lax record-keeping have made a hash of the underlying data.

“The federal government doesn’t really keep track of a lot of this equipment that goes to local law enforcement agencies,” says Anna Gunderson, a political scientist at Louisiana State University who coauthored a 2019 study that examined the effects of the 1033 program on crime rates. “The agencies themselves are inconsistent in keeping track. That just makes it really difficult for anyone to try to learn about the program or study it to try and analyze it, because we don’t have a very clear understanding what kinds of equipment actually are in the hands of these agencies.”

The LESO does maintain a spreadsheet detailing to whom it has distributed property over the years. When asked about complaints of inconsistent records, a spokesperson for the Defense Logistics Agency, which oversees LESO, noted that the agency changed accounting systems in 2013 to allow state coordinators and law enforcement agencies to identify and track what they receive. That switch, and spotty record-keeping beforehand, has confounded efforts to understand the impact of a program that has helped transform law enforcement in America.

“The DLA did not archive active inventories prior to 2014. They also did not archive information about transfers of equipment and destruction of controlled equipment during that

time. LEAs themselves typically only retain records for a few years, subject to their own local-level record keeping requirements," says Kenneth Lowande, a political scientist at the University of Michigan whose research includes the 1033 program. "Some of this can never be fixed. You can't recreate records that are lost."

The issues with 1033 have also run deeper than just contradictory or incomplete data sets. The Department of Defense does not provide training for law enforcement agencies that receive controlled property. Instead, it's left to recipients to certify their own training each year. "What programs like 1033 have done is given people the equipment to carry out operations that are traditionally done by tactical teams that otherwise would not have been able to obtain it," says Jonathan Mummolo, a political scientist at Princeton University who focuses on policing. "That is for sure not always accompanied by extensive training. There's just a lot of variation in policing standards across the board."

That seemingly lax oversight has manifested in other troubling ways, as well. In a 2017 sting operation, the General Accountability Office obtained over 100 controlled items from the 1033 program—including night-vision goggles and pipe bomb materials—with a total estimated value of $1.2 million. All it took was the creation of a fake law enforcement agency, website, and shipping address. The GAO's fraudulent application was processed and approved within a week.

The DLA implemented additional controls in the wake of the report, which focused on the acquisition process for federal law enforcement agencies rather than state and local. Those steps include a review of each existing applicant and establishing a point of contact at each federal agency to vet and approve requests. But the GAO's success in hoodwinking the agency did not inspire confidence. Nor has it inspired the federal government to fundamentally reconsider the premise of distributing controlled equipment to police in the first

place.

A year after Ferguson, then president Barack Obama signed an executive order that prohibited state and local law enforcement from receiving certain types of property, like grenade launchers and weaponized aircraft, under the 1033 program, but these restrictions were short-lived: Trump lifted them in 2017. Lowande argues the actual impact of that revocation has been negligible. Obama's original executive order ultimately only applied to around 300 departments, he says, and there's no sign in recent DLA inventories that previously restricted items have been sent out again. In a working paper currently under review, Lowande finds that the demilitarization efforts that did take place in those two years showed "no detectable impact on violent crime or officer safety."

"There is no compelling evidence, right now, that arming LEAs with military-grade equipment increases or decreases crime," he says.

Other research into the 1033 program, though, paints an alarming picture about its effect on police activity. "Our research suggests that officers with military hardware and mindsets will resort to violence more quickly and often," says Ryan Welch, a political scientist at the University of Tampa who coauthored a 2017 study on the effects of the 1033 program on police violence. "Other research shows that when governmental responses are violent, dissidents and protestors are more likely to act violently at the site and in the future. Of course, that leads to more violence from the government creating a spiral that is hard to escape."

In 2018, Princeton's Mummolo published research showing not only that special weapons and tactics teams are deployed more often in communities of color, but that they on average "provide no detectable benefits in terms of officer safety or violent crime reduction." Which is a point that often gets

lost: While the high-profile responses to police brutality demonstrations draw more attention to the 1033 program and others like it, in many parts of the country its impacts are a staple of policing.

“We tend to focus on these events when there’s massive social unrest and they’re dominating the headlines and we see militarized police come in, but militarized police are active in this country all the time,” says Mummolo. “It doesn’t take a situation like we’re seeing right now to activate them.”

This story originally appeared on wired.com.

https://arstechnica.com/?p=1680795

Employees, civil rights groups blast Facebook inaction on Trump statements

Enlarge / Thousands of peaceful demonstrators holding banners gather in front of the White House for the fifth consecutive day to protest the death of George Floyd, an unarmed black man who died after being pinned down by a white police officer in Minneapolis, on June 2, 2020 in Washington, DC, United States.

reader comments

105 with 60 posters participating

Share this story

As enormous protests in support of black communities and against police brutality continue to sweep across the United States, Facebook is facing a protest of its own. The company and its CEO, Mark Zuckerberg, are facing criticism from users, competitors, civil rights organizations, and even employees for allowing racist content and hate speech to proliferate on the platform, amplified by President Donald Trump.

Facebook on Tuesday removed some accounts affiliated with white supremacist groups after some members advocated bringing weapons to current protests, Reuters reports. It also removed accounts falsely claiming to be affiliated with antifascist groups that advocated stirring up trouble. Over the weekend, Twitter similarly removed accounts that were purporting to represent antifascist organizations but were in fact linked to a white nationalist group.

What Facebook has not taken action against, however, are statements by Trump or other public officials that also call for violence or stoke racism. Specifically, Facebook has declined to act against a post from May 29 in which Trump called protesters demonstrating following Minneapolis's police killing resident George Floyd "thugs." In the same post, the president added, "Any difficulty and we will assume control, but when the looting starts, the shooting starts."

Trump cross-posted the same message to both Facebook and Twitter. Last week, Twitter appended a label to the post explaining that Trump's message broke Twitter's rules against glorifying violence. The social media giant also added the label to a duplicate post by the official White House account featuring the same content, and it suspended an experimental account that repeated the president's tweets verbatim.

Even Snapchat has now taken action against Trump's account based on the content he posted to Facebook and Twitter. CEO

Evan Spiegel sent a memo to all employees on May 31 explaining that the platform will no longer be promoting the president's content in its Discover platform, writing, "we simply cannot promote accounts in America that are linked to people who incite racial violence, whether they do so on or off our platform."

Facebook employees promptly challenged Zuckerberg to do something. "Mark is wrong, and I will endeavor in the loudest possible way to change his mind," the leader of Facebook's News Feed design team said.

"I work at Facebook and I am not proud of how we're showing up," another Facebook employee said on Twitter. "The majority of co-workers I've spoken to feel the same way. We are making our voice heard."

Betrayal

One engineer publicly resigned from the company in protest. About three dozen of the company's earliest employees today signed on to a letter to Zuckerberg calling his choice a "betrayal" of the site's early ideals. "The company we joined valued giving individuals a voice as loud as their government's—protecting the powerless rather than the powerful," the former employees wrote. "Facebook isn't neutral, and it never has been. Making the world more open and connected, strengthening communities, giving everyone a voice—these are not neutral ideas. Fact-checking is not censorship. Labeling a call to violence is not authoritarianism. Please reconsider your position."

Facebook, like most other "knowledge sector" companies, currently has a majority of its employees working remotely due to the novel coronavirus crisis, and it plans to expand remote work going forward. Nonetheless, about 400 employees participated in a virtual walkout on Monday in protest of Facebook's inaction.

Zuckerberg defended his choices in an internal call with employees the next day. According to leaked audio of the call Recode obtained (transcript), Zuckerberg said he researched the Trump statement and found it "troubling," but he didn't see it violating the site's policies. "The reference is clearly to aggressive policing—maybe excessive policing—but it has no history of being read as a dog whistle for vigilante supporters to take justice into their own hands," Zuckerberg told said on the call.

During the call, Zuckerberg also admitted in response to employee questions that exactly one black Facebook employee had been involved in the company's decision. (Less than 4 percent of Facebook's US workforce are black.)

Civil rights, then and now

It is true that the phrase is not a dog whistle, which is something meant to sound innocuous to those who are not members of the target in-group. It is instead more of a megaphone, meant to be heard and amplified to everyone in range. It also does not instruct independent vigilantes to take action, but rather it encourages state and federal actors to do so.

The phrase originated with Miami Chief of Police Walter Headley in 1967. Headley, speaking about local unrest related to the civil rights movement, specifically said, "We don't mind being accused of police brutality… There is only one way to handle looters and arsonists during a riot and that is to shoot them on sight. I've let the word filter down: When the looting starts the shooting starts." Ardent segregationist George Wallace echoed the phrase during his failed 1968 presidential campaign.

Leaders of three civil rights groups—Color of Change, The Leadership Conference on Civil and Human Rights, and the NAACP Legal Defense and Educational Fund—also spoke with Zuckerberg

and Facebook COO Sheryl Sandberg about the company's choice not to act. The conversation did not go well. In a statement after the call, the directors of all three groups said they were "disappointed and stunned by Mark's incomprehensible explanations for allowing the Trump posts to remain up.

"He did not demonstrate understanding of historic or modern-day voter suppression and he refuses to acknowledge how Facebook is facilitating Trump's call for violence against protesters," they added. "Mark is setting a very dangerous precedent for other voices who would say similar harmful things on Facebook."

Rashad Robinson, president of Color of Change, also spoke with Bloomberg News about the call. "I feel like I spent a lot of time, and my colleagues spent a lot of time, explaining to him why these things are a problem, and I think he just very much lacks the ability to understand it," Robinson told Bloomberg.

Facebook's executive staff has been fully aware for years that the way its site operates stokes divisiveness and drives extremism, The Wall Street Journal recently reported.

As far back as 2016, Facebook's own internal research found that extremist content proliferated on the site, the WSJ found. A presentation delivered internally at the time found that "64% of all extremist group joins are due to our recommendation tools."

Rampant hate speech continues to proliferate all over Facebook, even as the company tries to increase its capacity to moderate content. So, too, does misinformation. Although Zuckerberg recently touted Facebook's ability to use fact-checking labels on false or misleading content related to COVID-19, he also refused to apply fact-checking to content posted by politicians.

Facebook and Zuckerberg have, in fact, explicitly said many times over that political figures—especially but not

exclusively the current US president—can break Facebook rules prohibiting hate speech and glorification of violence as much as they want, and the company won't do a thing about it.

Facebook certainly appears to be standing by that position. And changing that, it seems, may be as much of an uphill battle as everything else.

https://arstechnica.com/?p=1680837

Frontier users must pay "rental" fee for equipment they own until December

Enlarge / Don't worry, the fire isn't real.
Getty Images | RapidEye

reader comments

96 with 77 posters participating

Share this story

Broadband and TV providers can keep charging "rental" fees for equipment that customers own themselves until December 2020, thanks to a Federal Communications Commission ruling that delays implementation of a new law.

A law approved by Congress and signed by President Trump in December 2019 prohibits providers from charging device-rental

fees when customers use their own equipment, and it was originally scheduled to take effect on June 20. As we've written, this law will help Frontier customers who have been forced to pay $10 monthly fees for equipment they don't use and, in some cases, have never even received. But the law gave the FCC discretion to extend the deadline by six months if the commission "finds that good cause exists for such an additional extension," and the FCC has done just that.

The FCC ruling on April 3, which we didn't notice at the time, extends the deadline to December 20 and says that providers need more time to comply because of the coronavirus pandemic:

> *As the nation tackles the COVID-19 pandemic, multichannel video programming distributors (MVPDs) and providers of fixed broadband Internet access service are among the entities that are integral to the Commission's ongoing, nationwide effort to keep Americans informed and connected during this national emergency. So that these service providers may focus their resources on this critical effort, we provide appropriate flexibility for MVPDs and providers of fixed broadband Internet access service to fulfill their obligations under the Television Viewer Protection Act of 2019 (TVPA)… we find that good cause exists for granting a blanket extension of section 642's effective date until December 20, 2020.*

The new law, the FCC noted, "prohibits MVPDs and providers of fixed broadband Internet access service from charging consumers for equipment they do not provide." Compliance with the rental-fee provision and other billing-transparency requirements in the new law "may require that subject entities make changes to existing billing systems, provide employee training, or take other compliance measures, thereby requiring providers to divert resources away from other consumer demands brought on by the pandemic," the FCC said.

Frontier keeps charging rental fee

Last year, Frontier claimed that it charges the rental fee to cover higher support costs for customers who use their own routers, yet the company also said that it "cannot support or repair the non-Frontier equipment." Frontier is taking advantage of the extra six months and will keep charging its rental fee to customers who use their own equipment. A Frontier spokesperson told Ars today that the company "plans to comply with the requirements when the law goes into effect"—meaning in December. Unlike Frontier, other major ISPs usually let customers avoid rental fees when they use their own routers.

A Frontier customer in Florida named John emailed Ars this week after he asked Frontier if the company would stop charging the fee in June. We agreed to publish only first names for John and another customer quoted later in this article. John told us:

> *I called Frontier's Florida customer service office yesterday, requesting the procedure to mail back the Frontier router in preparation of the new law going into effect, and the representative stated that I would still be charged for the rental because, I quote, "Frontier requested a 6-month extension to the January ruling and it was approved. As a result, you will continue to be charged the $10/month until December [2020]."*

The Frontier spokesperson told Ars that the company "did not request an exemption," although a trade group that represents Frontier did ask for an industry-wide exemption. Either way, it's disappointing for customers that the FCC granted the exemption and that Frontier will take advantage of it.

"You and I both know this has more to do with retaining revenues than it does with a provider's ability to 'comply'

with the new law due to COVID-19," John told Ars.

"Considering Frontier's recent bankruptcy filing, I'm not surprised they are continuing to stick it to their clients," John also said. "Bottom line: Don't advertise the service in large font as a $39.99/month service if it is *mandatory* you pay their $10/month rental fee."

Other customers have slightly better luck

We also heard from a customer in Oregon, one of four states where Frontier recently sold its network to a company doing business as Ziply Fiber. The Oregon customer, Phillip, says Ziply agreed to take the $10 router-rental charge off his bill—but not right away. Phillip bought his own router and returned the company-provided one to Ziply. But Ziply kept putting the $10 charge on his bills.

Phillip spoke to a customer service rep who tried to remove the router fee, "but the system would not let him," Phillip told us. Phillip says he then talked to a supervisor and pointed out the new US law prohibiting these charges.

"I quoted your article and the law to the supervisor and she said they would put in a ticket to the appropriate team to update the software so they could actually remove the equipment," Phillip told us in an email. "She then told me that it would take ~2 bills for that to be done and… she said I would need to call in each time I got a bill with the fee listed to have it manually removed."

Rich Son, a Frontier customer in Texas who we wrote about last year, told us today that "Frontier stealthily removed the charge from my account" about a month after that story was published. But with other Frontier customers still facing the charge, Son told Ars that "It's hard for me to believe that

removing one line item would take six months to accomplish, pandemic or not.”

FCC agreed with industry lobbyists

Despite using COVID-19 as cover to force customers to keep paying fees for nonexistent equipment, the FCC has urged ISPs to voluntarily waive late fees and not disconnect customers who can’t pay because of the pandemic. Of course, letting customers save money by nixing unnecessary rental fees would also help people struggling during the pandemic, but the FCC order granting the extension did not mention that.

The FCC granted the extension after being urged to do so by three major cable and telecom trade groups. One of those groups is USTelecom, of which Frontier is a member. The groups said they planned to ask for the extension even before the pandemic shut down much of the US economy. The trade groups told the FCC on March 26:

> *Under ordinary circumstances, the initial six-month effective date would not have allowed enough time for cable operators and other multichannel video programming distributors (MVPDs) to come into compliance with the various provisions of the Act, and an extension to December 20, 2020 would be justified based on that reason alone. The COVID-19 pandemic has now made compliance by the current June 20, 2020 effective date virtually impossible, as resources once thought available for this purpose must now be redirected toward meeting the needs of customers impacted by virus. Indeed, the continuing crisis may jeopardize compliance even if a six-month extension is granted.*
>
> *The pandemic is consuming available resources for our members across all divisions of their business, including the teams that provide production, development and customer support for TVPA implementation. For example, one immediate COVID-19 impact is reduced capacity at members’ customer call centers.*

> *Having to create new scripts, conduct training, and learn new routines around the new TVPA requirements would be an additional burden at a time when members' resources in customer care are already strained. In addition, as call center operations become disrupted, members are working to develop more online self-care resources and functions, which requires significant development work.*

Besides the equipment-rental provision, the new law includes several provisions that should make it harder for providers to mislead customers about prices. For example, a new right to transparency requires TV and broadband companies to provide customers the total monthly charges—including all company-imposed fees and a good-faith estimate of all government-imposed fees and taxes—before customers enter into a contract. This notice must also specify the amount of promotional discounts and when those discounts will expire. When it finally takes effect, the law is supposed to give consumers 24 hours to cancel without penalty after entering a contract.

https://arstechnica.com/?p=1680905

COVID-19 privacy protection bill introduced with bipartisan support

Enlarge / A global pandemic is no excuse for sticking your nose in other people's private data.

reader comments

50 with 33 posters participating

Share this story

A group of lawmakers from both parties is putting forth legislation that aims to protect Americans' privacy and personal data while advancing public health initiatives in the face of COVID-19.

Well over 100,000 people in the United States have died as a result of the current pandemic, which is far from over. Mitigating the further spread of the disease will require robust contact tracing, among other efforts. The scale of tracing required, however, is enormous and difficult to manage.

In the modern era, any issue of scale is met with the promise of an app, and contact tracing is no different. Apple and Google worked together on an API for contact tracing, which was recently deployed to phones. But public confidence in contact-tracing apps is already mixed at best, and recent statements by state and local governments conflating public health contact tracing with police investigation of protesters have sown further distrust.

A proposed bill, called the Exposure Notification Privacy Act (PDF), seeks to limit what data entities collecting COVID-19 exposure data can collect and how they can use it.

The Act would first require all contact tracing to be opt-in only, requiring "affirmative express consent." The text specifically mandates that every user of an app would have to consent clearly and voluntarily, rather than just having consent inferred from "continued use of a service or product," as so many platforms currently do.

Operators of such apps would also be required not only to

gather the minimum amount of user information necessary and de-identify aggregate data but also to promise not to combine it with other data in order to identify "any individual or device." App makers would also be required to use the data they gather for public health purposes only, not for any commercial purpose, and any entity to which they might transfer user data would be required to adhere to the same conditions.

Senators Maria Cantwell (D-Wash.) and Bill Cassidy (R-La.) together introduced the bill, with Sen. Amy Klobuchar (D-Minn.) signing on as a co-sponsor.

"Public health needs to be in charge of any notification system so we protect people's privacy and help them know when there is a warning that they might have been exposed to COVID-19," Cantwell said in her written statement. She also told the Washington Post she's not inclined to use contact tracing apps without such permissions in place, adding, "We're all irritated our browser history might be sold a thousand times over, but when it's your healthcare history, it's a whole new realm."

Cassidy echoed the sentiment to the Post, saying, "I think if you ask most people, 'Do you trust Google to respect your privacy?'" the answer is no. "This is a matter of perception. It's not an indictment of Google; we're making sure people are comfortable with this."

Several public health and digital rights experts and advocates endorsed the bill, expressing hope it could help technologists and public health officials strike the right balance of increasing public safety while protecting privacy.

This isn't the first stab Congress has taken at a coronavirus-specific privacy bill, but it is the first such effort to hit the ground running with at least some support from both parties. The Public Health Emergency Privacy Act, introduced

in May, has Democratic backers in both the House and Senate but is unlikely to win Republican support. That proposal followed an earlier bill, the COVID-19 Consumer Data Protection Act, which was put forth by Senate Republicans and is unlikely to win Democratic support.

https://arstechnica.com/?p=1680625

AT&T exempts HBO Max from data caps but still limits your Netflix use

Enlarge / AT&T executive John Stankey at a presentation for investors at Warner Bros. Studios on October 29, 2019, in Burbank, California.

reader comments

70 with 63 posters participating

Share this story

AT&T's new HBO Max streaming service is exempt from the carrier's mobile data caps, even though competing services such as Netflix, Amazon, and Disney+ count against the monthly data limits. This news was reported today in an article by The Verge, which said that AT&T "confirmed to The Verge that HBO Max will be excused from the company's traditional data caps and the soft data caps on unlimited plans."

The traditional data caps limit customers to a certain amount of data each month before they have to pay overage fees or face extreme slowdowns for the rest of the month. “Soft data caps on unlimited plans” apparently is a reference to the 22GB or 50GB thresholds, after which unlimited-data users may be prioritized below other users when connecting to a congested cell tower.

“According to an AT&T executive familiar with the matter, HBO Max is using AT&T’s ‘sponsored data’ system, which technically allows any company to pay to excuse its services from data caps,” The Verge wrote. “But since AT&T owns HBO Max, it’s just paying itself: the data fee shows up on the HBO Max books as an expense and on the AT&T Mobility books as revenue. For AT&T as a whole, it zeroes out. Compare that to a competitor like Netflix, which could theoretically pay AT&T for sponsored data, but it would be a pure cost.”

We asked AT&T whether HBO Max will also be exempt from AT&T home-Internet data caps and will update this article if we get an answer. (**Update**: AT&T told us the new streaming service is not exempt from home-Internet caps, so “HBO Max would count toward your home data allotment.”) AT&T home and mobile data caps are suspended during the coronavirus pandemic until at least June 30, but AT&T will presumably bring them back sometime after that.

AT&T is including HBO Max at no extra charge on certain Internet plans, which it also did with previous versions of HBO.

Pai’s FCC green-lit zero-rating

AT&T has owned HBO since it purchased Time Warner in June 2018. HBO Max, which costs $15 a month, is essentially an expansion of the HBO Now service. The HBO Max user interface did not impress Ars reviewer Sam Machkovech when he tested it out last week.

- AT&T customers won’t need to burn through their data plans to scroll through HBO Max’s unwieldy interface, which Ars Technica’s Sam Machkovech likened to “crashing through the glass door of a badly managed Blockbuster Video.”
- HBO Max’s hubs.
- The 25 series in the Cartoon Network hub, as of launch.
- A visit to the Sesame Street hub reveals a peculiar organizational issue: categories that link to entire episodes. Those “spoofs and parodies” are tucked into longer episodes, and HBO Max doesn’t use timestamps to let watchers skip directly to the relevant bits. It’s an unwieldy attempt to guide viewers.
- The 9 series in the Adult Swim hub, as of launch.
- You have to scroll quite a ways to pick through more episodes, though at least the season-skipping interface is nimble enough.
- When watching videos on a desktop Web browser, the interface largely resembles HBO Now, complete with the “rewind 15 seconds” button. You won’t find that convenient toggle on every platform, however.
- The opening page for any series has a *massive* sample screen.

When Democrat Tom Wheeler chaired the Federal Communications Commission, the agency ruled that AT&T and Verizon Wireless violated net neutrality rules by letting their own video services stream without counting against customers’ mobile data caps while charging other video providers for the same data cap exemptions. In that case, AT&T was letting DirecTV services stream without counting against the cap. The FCC rescinded the finding less than two weeks after President Trump promoted Republican Ajit Pai to the chairmanship, and carriers have since been free to deploy data-cap exemptions as they wish.

In July 2015, when AT&T bought DirecTV, the Wheeler FCC

imposed a merger condition that barred AT&T from exempting its own online video services from home-Internet data caps. But the condition had a four-year time limit and expired in 2019, and the condition never applied to AT&T's mobile network.

https://arstechnica.com/?p=1680630

Lawsuit over online book lending could bankrupt Internet Archive

Enlarge / The book drop outside the Spring Township library in Pennsylvania was closed on April 6, 2020.

reader comments

87 with 62 posters participating

Share this story

Four of the nation's leading book publishers have sued the Internet Archive, the online library best known for maintaining the Internet Wayback Machine. The Internet Archive makes scanned copies of books—both public domain and under copyright—available to the public on a site called the Open Library.

"Despite the Open Library moniker, IA's actions grossly exceed legitimate library services, do violence to the Copyright Act, and constitute willful digital piracy on an industrial scale,"

write publishers Hachette, HarperCollins, Wiley, and Penguin Random House in their complaint. The lawsuit was filed in New York federal court on Monday.

For almost a decade, the Open Library has offered users the ability to "borrow" scans of in-copyright books via the Internet. Until recently, the service was based on a concept called "controlled digital lending" that mimicked the constraints of a conventional library. The library would only "lend" as many digital copies of a book as it had physical copies in its warehouse. If all copies of a book were "checked out" by other patrons, you'd have to join a waiting list.

In March, as the coronavirus pandemic was gaining steam, the Internet Archive announced it was dispensing with this waiting-list system. Under a program it called the National Emergency Library, IA began allowing an unlimited number of people to check out the same book at the same time—even if IA only owned one physical copy.

Before this change, publishers largely looked the other way as IA and a few other libraries experimented with the digital lending concept. Some publishers' groups condemned the practice, but no one filed a lawsuit over it. Perhaps the publishers feared setting an adverse precedent if the courts ruled that CDL was legal.

But the IA's emergency lending program was harder for publishers to ignore. So this week, as a number of states have been lifting quarantine restrictions, the publishers sued the Internet Archive.

In an email to Ars Technica, IA founder Brewster Kahle described the lawsuit as "disappointing."

"As a library, the Internet Archive acquires books and lends them, as libraries have always done," he wrote. "Publishers suing libraries for lending books, in this case, protected digitized versions, and while schools and libraries are

closed, is not in anyone's interest."

"The publishers have a pretty strong case"

The publishers' legal argument is straightforward: the Internet Archive is making and distributing copies of books without permission from copyright holders. That's generally illegal unless a defendant can show it is authorized by one of copyright law's various exceptions.

Legal experts tell Ars that the Internet's Archive's best response is to argue that its program is fair use. That's a flexible legal doctrine that has been used to justify a wide range of copying over the decades—from recording television broadcasts for personal use to quoting a few sentences of a book in a review. Most relevant for our purposes, the courts have held that it is a fair use to scan books for limited purposes such as building a book search engine.

When considering a fair use claim, courts consider several factors, including the impact of the use on the market for the original work. A book search engine, for example, is not a substitute for reading books but, rather, helps readers find new books they might want to buy. This is one of the reasons the courts found that book scanning for a search engine was legal under fair use.

But it's harder to come up with compelling arguments that the Internet Archive's open-ended lending program is fair use.

James Grimmelmann, a copyright scholar at Cornell University, told Ars that he is withholding judgment until he sees the Internet Archive's response. However, he said, "it seems like the publishers have a pretty strong case."

"I think there are arguments for fair use, but they're not terribly strong arguments," he said in a Monday phone

interview.

A pandemic exception?

The Internet Archive would have had a stronger argument if it had continued to limit the number of copies that could be lent out. In that scenario, IA could argue that the program's impact on the market was little different from a conventional library.

Obviously, a patron who checks out a book from a library is less likely to purchase a copy, undermining the market for the book. On the other hand, libraries themselves buy many books—and the more popular a book is, the more copies libraries must buy. So the overall impact of libraries on demand for books is not clear.

But once the IA stopped buying a copy of a book for every copy it lent out, this argument became a lot weaker. An institution like AI can buy a single copy of a book and then "lend" it to dozens, hundreds, or thousands of people at the same time. There's little doubt that this has a negative impact on the market for new books.

Instead, the Internet Archive will likely need to make a more novel argument—that the unique circumstances of a pandemic justifies allowing types of infringement that would be clearly illegal at other times. Grimmelmann wasn't able to identify any other cases where courts have made that kind of leap.

I also spoke to John Bergmayer, a copyright expert at the copyright reform group Public Knowledge. He said there was a "pretty strong fair use argument" for both the Internet Archive's previous controlled digital lending program and its new approach without waiting lists. Bergmayer pointed to the fact that millions of books are currently locked up in libraries that have been closed due to the pandemic. That, he said, creates a unique situation that could justify digital

lending activities that would otherwise be illegal.

But like Grimmelmann, Bergmayer couldn't name any specific court decisions that back up IA's aggressive interpretation of copyright law.

The stakes are high

While Grimmelmann was fairly bullish on the publishers' legal prospects, he disagreed with one aspect of the industry's argument. The Internet Archive is officially a non-profit, but the publishers' lawsuit portrays the group as effectively a commercial operation profiting from copyright infringement. It points out that IA has earned millions of dollars from contracts to scan books on behalf of partners such as other libraries.

But Grimmelmann told Ars that this fundamentally misunderstands the motivations of Brewster Kahle, the founder of Internet Archive and still its driving force.

"Brewster Kahle is what the Russians might call a holy fool—someone who acts without real regard for himself or for worldly things in the service of a higher calling," Grimmelmann said. The Internet Archive "is not a commercial venture," he argued. Grimmelmann believes that Kahle, a 1990s dot-com entrepreneur who has sunk millions of dollars into the Internet Archive, is fundamentally an idealist.

But Kahle's idealism—or foolishness—might cost him dearly. Copyright law allows statutory damages as high as $150,000 per work for willful infringement. And Grimmelmann tells Ars that if the publishers win the case, they'll have a strong case that the infringement was willful.

The Internet Archive has scanned more than a million books that are still under copyright, so a loss could easily lead to billions of dollars in damages—far beyond the non-profit's

ability to pay. So if the publishers win the lawsuit, they could force the Internet Archive out of business. That would be an incalculable loss given the group’s work archiving other types of content, including the early Web.

However, the publishers may not be interested in forcing the Internet Archive out of business. Their goal is to get the Internet Archive to stop scanning their books. If they win the lawsuit, they might force the group to shut down its book scanning operation and promise to not start it up again, then allow it to continue its other, less controversial offerings.

https://arstechnica.com/?p=1680461