# Police use of facial recognition violates human rights, UK court rules

Enlarge / A close-up of a police facial recognition camera in use at the Cardiff City Stadium on January 12, 2020 in Cardiff, Wales. Police used the technology to identify individuals who were issued with football banning orders in an attempt to prevent disorder. Critics argued that the use of such technology is invasive and discriminatory.

## reader comments

54 with 39 posters participating

## Share this story

Privacy advocates in the UK are claiming victory as an appeals court ruled today that police use of facial recognition technology in that country has “fundamental deficiencies” and violates several laws.

South Wales Police began using automated facial recognition technology on a trial basis in 2017, deploying a system called AFR Locate overtly at several dozen major events such as soccer matches. Police matched the scans against watchlists of known individuals to identify persons who were wanted by the police, had open warrants against them, or were in some other way persons of interest.

In 2019, Cardiff resident Ed Bridges filed suit against the police, alleging that having his face scanned in 2017 and 2018 was a violation of his legal rights. Although he was backed by UK civil rights organization Liberty, Bridges lost his suit in

2019, but the Court of Appeal today overturned that ruling, finding that the South Wales Police facial recognition program was unlawful.

“Too much discretion is currently left to individual police officers,” the court ruled. “It is not clear who can be placed on the watchlist, nor is it clear that there are any criteria for determining where AFR can be deployed.” The police did not sufficiently investigate if the software in use exhibited race or gender bias, the court added.

The South Wales Police in 2018 released data admitting that about 2,300 of nearly 2,500 matches—roughly 92 percent—the software made at an event in 2017 were false positives.

“I’m delighted that the Court has agreed that facial recognition clearly threatens our rights,” Bridges said in a written statement after the ruling. “This technology is an intrusive and discriminatory mass surveillance tool… We should all be able to use our public spaces without being subjected to oppressive surveillance.”

The ruling did not completely ban the use of facial recognition tech inside the UK, but does narrow the scope of what is permissible and what law enforcement agencies have to do to be in compliance with human rights law.

“I am confident this is a judgment that we can work with,” a spokesperson for the South Wales Police said, confirming that the agency does not plan to challenge the ruling.

## Widespread impact?

Other police inside the UK who deploy facial recognition technology will have to meet the standard set by today’s ruling. That includes the Metropolitan Police in London, who deployed a similar type of system earlier this year.

Liberty hailed the victory as “the world’s first legal

challenge” to police use of facial recognition tech, but it’s almost certainly not going to be the last. Police use of facial recognition technology here in the United States has come under increased scrutiny against the backdrop of this year’s nationwide civil rights protest movement in support of Black communities and against police brutality.

The ACLU in June filed a formal complaint, though not a lawsuit, against police in Detroit after they arrested the wrong man based on a false-positive match from a facial ID system. That system, the Detroit police chief later admitted, misidentifies suspects a whopping 96 percent of the time.

The US companies that manufacture facial recognition systems have also tried to distance themselves from police in recent months. IBM left the business entirely in June; CEO Arvind Krishna said at the time, “vendors and users of AI systems have a shared responsibility to ensure that AI is tested for bias, particularly when used in law enforcement, and that such bias testing is audited and reported.” A few days later, Amazon followed suit with a one-year moratorium on allowing police to use its facial recognition platform, Rekognition.

https://arstechnica.com/?p=1698159

---

# Charter tries to convince FCC that broadband customers want data caps

## reader comments

140 with 110 posters participating

## Share this story

Charter Communications has claimed to the Federal Communications Commission that broadband users enjoy having Internet plans with data caps, in a filing arguing that Charter should be allowed to impose caps on its Spectrum Internet service starting next year.

Charter isn't currently allowed to impose data caps because of conditions the FCC placed on its 2016 purchase of Time Warner Cable. The data-cap condition is scheduled to expire on May 18, 2023, but Charter in June petitioned the FCC to let the condition expire two years early, in May 2021.

With consumer-advocacy groups and Internet users opposing the petition, Charter filed a response with the FCC last week, saying that plans with data caps are "popular."

"Contrary to Stop The Cap's assertion [in an FCC filing] that consumers 'hate' data caps, the marketplace currently shows that broadband service plans incorporating data caps or other usage-based pricing mechanisms are often popular when the limits are sufficiently high to satisfy the vast majority of users," Charter told the FCC.

Charter's filing continued:

> *There is also evidence that some consumers—either those who do not consume a lot of data and/or those who are looking for a lower-cost plan—may want a service where prices are based on the amount of data used… These different plans are proliferating in the market because they offer consumers a cost-effective alternative to unlimited data plans that are more than adequate to meet their needs. The DC/UBP [data caps and usage-based pricing] Condition, however, prevents Charter*

> *from keeping pace with its competitors and offering consumers the kinds of plans they are looking for. While Charter sees value in providing its service without data caps or UBP and has no plans to change that practice, Charter reasonably seeks the same flexibility that all of its competitors and peers have to manage data usage. This way if circumstances change, it has flexibility to offer the service packages its customers want.*

Charter neglected to mention that home-Internet providers generally don't charge customers less when they don't use much data. Instead, the price is usually the same regardless of whether one uses 10GB a month or 1.2TB. Cable customers who exceed a data cap have to pay extra fees, but aside from some limited exceptions, they don't get a discount off the base price when they stay under the cap.

Charter pointed to Comcast's 1.2TB monthly data cap and the fact that most customers don't use that much data as evidence that "the market does not support unreasonable data limitations." But Comcast—like Charter—is the only high-speed cable or fiber provider for tens of millions of customers across the United States, so Comcast customers don't have much choice. Comcast imposes its cap in most of the states it operates in, but not in the Northeast US where it faces strong competition from Verizon's un-capped fiber-to-the-home FiOS service—evidence that "the market" discourages caps when ISPs face real competition.

Charter also claimed the merger condition "prevents Charter from developing innovative service plans that are more tailored to consumers' needs," but there is nothing preventing Charter from offering cheaper plans to customers now and differentiating plans by speed instead of data allotment. In fact, Charter already does that by charging different prices for different speeds and by offering a low-cost plan with 30Mbps speeds to low-income families.

## Charter: Lack of competition is “beside the point”

Charter’s petition also asks the FCC to lift a condition that prevents the company from charging network-interconnection fees to large online video providers.

Charter claimed that it faces sufficient competition from wireline, mobile, and satellite providers. But Charter also argued that “Opponents’ claims that the [broadband] market is not competitive are beside the point… because Charter, like other broadband providers, lacks the incentive or ability to discriminate against OVDs [online video distributors]. OVDs are critical to the [broadband] business and far too large and powerful to thwart with data caps or interconnection fees.”

Charter’s petition said that in June this year, “residential data usage for Internet-only customers was 600 gigabytes per month, up nearly 20 percent from the fourth quarter of 2019 due to pandemic-related working and learning from home.”

## Roku: Data caps should be “a relic of the past”

Charter’s petition is opposed by consumer advocates, hundreds of customers who submitted filings to the FCC docket, and Roku.

“If it were to sanction data caps in the absence of competitive broadband Internet access services, the Commission would not only allow Charter to act on its incentives to act anti-competitively but also signal to other broadband providers who are unconstrained by competition that they too are free to adopt anti-competitive measures. Data caps should become a relic of the past,” Roku told the FCC last week.

Charter also faces opposition from Incompas—an industry group

that represents Netflix, Amazon, other online service providers—and a variety of companies in the telecom business. Charter has gotten support for its petition from charities and politicians it donated to, as we detailed in a previous article.

But Charter apparently wrote letters on behalf of charities, and one of the groups has said it doesn't actually support Charter's petition, Bloomberg reported yesterday:

> *When asked by Bloomberg News about a letter filed July 20, the Niagara Falls Boys & Girls club, which got $5,000 from Charter for a summer camp, backed away from its support for the measure Charter is seeking from the FCC.*
>
> *The letter the club submitted was prepared by Charter and "upon closer review, the last paragraph of the letter states that we support" Charter's request, Rebecca Vincheski, chief executive officer of the club, said in an email.*
>
> *The club has "a position of neutrality on this important community issue," Vincheski said.*

The deadline for submitting responses to Charter's petition passed on August 6. FCC Chairman Ajit Pai voted against the merger conditions when they were imposed in 2016 under then-FCC Chairman Tom Wheeler and could ask the Republican-majority commission to vote on Charter's petition in the coming months.

*Disclosure: The Advance/Newhouse Partnership, which owns 13 percent of Charter, is part of Advance Publications. Advance Publications owns Condé Nast, which owns Ars Technica.*

https://arstechnica.com/?p=1698198

# NJ Supreme Court: No 5th Amendment right not to unlock your phone

ymgerman / Getty

## reader comments

125 with 86 posters participating, including story author

## Share this story

New Jersey’s Supreme Court has ruled that compelling a suspect to unlock his or her cell phone doesn’t violate the Fifth Amendment. The courts continue to be deeply split on this question. Back in June, Indiana’s Supreme Court reached the opposite conclusion, and several other state and federal courts have reached divergent positions on the issue over the last few years.

This case focuses on an allegedly corrupt cop named Robert Andrews. Andrews is a former Essex County Sheriff who allegedly tipped off a suspect named Quincy Lowery about a pending police investigation. Under police questioning, Lowery testified that Andrews had advised him to get a new phone to avoid a police wiretap. He also said Andrews helped Lowery identify an undercover police officer and an unmarked police vehicle. These allegations were corroborated by data from Lowery’s phone.

The police seized two iPhones belonging to Andrews, but investigators were unable to unlock them. Andrews refused to unlock the phones based on the Fifth Amendment, which protects

against self-incrimination.

On Monday, the New Jersey Supreme Court rejected that Fifth Amendment claim. The Fifth Amendment only protects defendants against self-incriminating *testimony*, not the production of incriminating documents. While "testimony" usually refers to speech, that's not always the case. Sometimes, a defendant can reveal information by his or her actions. For example, if the government doesn't already know who owns a phone, then forcing a defendant to unlock it amounts to forced testimony that the defendant is the owner.

But that reasoning doesn't apply in this case. The phones were registered in Andrews' name and were in his possession. There's little doubt that Andrews knows the passcodes. So if he's forced to enter the passcodes to his own phones, the New Jersey Supreme Court reasoned, he's not revealing any information that the government doesn't already know.

Of course, the information *on* the phone may be incriminating. But the courts have long held that forced production of documents—even incriminating ones—is not a violation of the Fifth Amendment. The government can order a defendant to unlock a safe even if the safe might have incriminating documents inside of it.

# The other side

As we mentioned before, the Indiana Supreme Court took the opposite view just two months ago. And as I wrote at the time, that was just the latest example of a deep divide among courts on this issue:

> *Earlier this year, a Philadelphia man was released from jail after four years of being held in contempt in connection with a child-pornography case. A federal appeals court rejected his argument that the Fifth Amendment gave him the right to refuse to unlock hard drives found in his possession.*

> *A Vermont federal court reached the same conclusion in 2009—as did a Colorado federal court in 2012, a Virginia state court in 2014, and the Massachusetts Supreme Judicial Court in 2014.*
>
> *But other courts in Florida, Wisconsin, and Pennsylvania have reached the opposite conclusion, holding that forcing people to provide computer or smartphone passwords would violate the Fifth Amendment.*

Courts that have found the Fifth Amendment does shield defendants against unlocking their phones have focused not on the passcodes but on the information contained in the phone. They point to a 2000 ruling in the prosecution of Bill Clinton business associate Webster Hubbell for tax fraud. Prosecutors had ordered Hubbell to provide documents in several broad categories. The Supreme Court ruled that this violated the Fifth Amendment because Hubbell wasn't just being asked to turn over particular documents—he was using his own judgment to decide which documents fell into the broad categories the government asked about.

Courts like the Indiana Supreme Court have concluded that similar reasoning applies in cell phone unlocking cases. Governments aren't seeking specific files on a suspect's device, they're seeking unfettered access to a suspect's cell phone, giving them access to information they might not have known existed previously. Some courts have held that this kind of fishing expedition is analogous to the broad document requests in the *Hubbell* case.

But in Monday's ruling, the New Jersey supreme courts pointed out a key difference: Hubbell was required to use his own knowledge and judgments to decide which documents to turn over. That compelled exercise of judgment—not just the fact that the government might get incriminating documents it didn't know about before—was what made Hubbell's response

self-incriminating testimony. By contrast, unlocking a cell phone doesn't require a suspect to make any judgments about the information on the cell phone.

The New Jersey Supreme Court points out that there's a different constitutional provision that's supposed to protect the privacy of people's private data. That's the Fourth Amendment, which protects "papers" against "unreasonable searches and seizures." The New Jersey Supreme Court argues that focusing on the phone's contents, rather than on the production of the passcode itself, "imports Fourth Amendment privacy principles into a Fifth Amendment inquiry." If the police are engaging in improper fishing expeditions, the way to deal with that is by challenging the search warrant on Fourth Amendment grounds.

Ultimately, the only way to resolve this dispute is for the US Supreme Court to get involved. The high court hasn't ruled on the legality of compelled decryptions of smartphones or other digital devices. Indeed, most of the Fifth Amendment caselaw in this era predates smartphones—and in many cases the personal computer, too. It would be helpful for the nation's highest court to take this issue on and provide clarity to courts that are struggling with how to apply these decades-old precedents.

https://arstechnica.com/?p=1698156

---

# HS that suspended teen who tweeted photo of hallway has

# 9 COVID-19 cases

Enlarge / Photo from North Paulding High School, tweeted by student Hannah Watters on Tuesday, August 4.

## reader comments

240 with 118 posters participating

## Share this story

There are nine newly confirmed COVID-19 cases at the high school that suspended a 15-year-old who had tweeted a photo of a hallway packed with maskless students.

North Paulding High School in Dallas, Georgia sent a letter to parents Saturday, saying, “At this time, we know there were six students and three staff members who were in school for at least some time last week who have since reported to us that they have tested positive.” The letter was published by the Atlanta Journal-Constitution.

Most or even all of the six students and three staff members who tested positive could have had the virus before the school reopened on Monday, August 3. As Harvard Medical School explains, “The time from exposure to symptom onset (known as the incubation period) is thought to be three to 14 days, though symptoms typically appear within four or five days after exposure,” and “a person with COVID-19 may be contagious 48 to 72 hours before starting to experience symptoms.”

But regardless of when those nine people were infected, their presence at a school where hallways were packed with students not wearing masks means that many other students and teachers were placed at risk of infections that could show up in test results in the near future. The high school has about 2,000

students.

Even before the reopening, some members of the high school football team had already tested positive for COVID-19. “Paulding County Schools have reported a total of 53 cases of coronavirus within the district since July 1,” including 23 at the high school, according to Channel 2 in Atlanta.

As we reported Friday, the school issued a 5-day suspension to student Hannah Watters after she posted a photo to Twitter, noting the “jammed” hallways and “10 percent mask rate.” The school lifted her suspension after extensive media coverage. One other unnamed student who was suspended for a similar reason also had the suspension reversed, the Journal-Constitution said.

Students attended class in person only on Monday through Wednesday, as the district said it conducted a short first week “so that all of our schools can step back and assess how things are going so far.”

**Update at 6:50pm ET:** North Paulding High School announced Sunday that it has canceled in-person instruction for Monday and Tuesday, August 10 and 11, because of the nine positive cases and “the possibility that number could increase if there are currently pending tests that prove positive.” The school said that on Tuesday evening, parents and students will be notified about whether in-person instruction will resume on Wednesday. Remote learning will continue while the school is closed.

## “They sat in class all day long with no masks”

The Journal-Constitution provided details on some of the students who tested positive:

> *Angie Franks said both her nephews who attend the school have*

> *tested positive for COVID-19. One came home from school Monday unable to smell, she said in an interview with the AJC. His mother took him for testing and the results the next day showed him positive, Franks said. By then, his brother was exhibiting symptoms and was also tested. His positive results were returned Wednesday.*
>
> *The students are quarantining at home, but both went to school Monday. Franks said the boys' father notified the school on Tuesday and Wednesday after getting their test results.*
>
> *"They sat in class all day long with no masks and not social distancing," Franks said. "And I have no idea how many kids they came into contact with."*
>
> *She said the boys didn't grasp the gravity of the virus and weren't encouraged to wear masks in classrooms or hallways by the school. Paulding County's school system is not mandating masks for students and staff, though it is supplying them for teachers.*

An elementary school nurse who worked in another school in Paulding County told the Journal-Constitution that she resigned from her job last month because of insufficient pandemic policies including the lack of a mask mandate.

## School is being cleaned

The high school's letter to parents on Saturday said that "Our custodial staff continues to thoroughly clean and disinfect the school building daily, and especially affected areas." But as the Journal-Constitution noted, "The letter to parents does not include information on whether any other students or staff who were exposed have to quarantine or whether any classrooms will be closed."

The letter recommends checking children's temperature at least

twice a day and checking for a list of COVID-19 symptoms. “If your child exhibits any of these COVID-19 symptoms, the CDC and DPH recommend your child be tested as soon as possible. In addition, please notify the school front office as it is imperative that students who are showing symptoms stay home and quarantine,” the letter said.

In Sunday’s update to parents, the school said that after further cleaning on Monday and Tuesday, the district will “consult with the state Department of Public Health to assess the [school] environment and determine if there are any additional close contacts for confirmed cases who have not already been identified.” People who tested positive and close contacts must quarantine for 14 days before returning to school, the new update said.

“The health and wellbeing of our staff and students remains our highest priority, and we are continuing to adjust and improve our protocols for in-person instruction to make our school the safest possible learning environment,” the letter yesterday said.

Elsewhere in Georgia, Atlanta Public Schools decided to postpone opening until August 24 and to impose a mask mandate. Georgia Governor Brian Kemp has tried to stop cities and towns from imposing mask mandates.

https://arstechnica.com/?p=1697730

---

# Bill Gates on COVID-19: Most

# US tests are “completely garbage”

Enlarge / Despite trillions of dollars of economic damage, Bill Gates is optimistic that a strong pipeline of therapies and vaccines will carry the US through the pandemic.
Jeff Pachoud | Getty Images

## reader comments

193 with 106 posters participating

## Share this story

For 20 years Bill Gates has been easing out of the roles that made him rich and famous—CEO, chief software architect, and chair of Microsoft—and devoting his brain power and passion to the Bill and Melinda Gates Foundation, abandoning earnings calls and antitrust hearings for the metrics of disease eradication and carbon reduction. This year, after he left the Microsoft board, one would have thought he would have relished shedding the spotlight directed at the four CEOs of big tech companies called before Congress.

But as with many of us, 2020 had different plans for Gates. An early Cassandra who warnedof our lack of preparedness for a global pandemic, he became one of the most credible figures as his foundation made huge investments in vaccines, treatments, and testing. He also became a target of the plague of misinformation afoot in the land, as logorrheic critics accused him of planning to inject microchips in vaccine recipients. (Fact check: false. In case you were wondering.)

My first interview with Gates was in 1983, and I’ve long lost count of how many times I’ve spoken to him since. He’s yelled

at me (more in the earlier years) and made me laugh (more in the latter years). But I've never looked forward to speaking to him more than in our year of Covid. We connected on Wednesday, remotely of course. In discussing our country's failed responses, his issues with his friend Mark Zuckerberg's social networks, and the innovations that might help us out of this mess, Gates did not disappoint. The interview has been edited for length and clarity.

**WIRED:** You have been warning us about a global pandemic for years. Now that it has happened just as you predicted, are you disappointed with the performance of the United States?

**Bill Gates:** Yeah. There's three time periods, all of which have disappointments. There is 2015 until this particular pandemic hit. If we had built up the diagnostic, therapeutic, and vaccine platforms, and if we'd done the simulations to understand what the key steps were, we'd be dramatically better off. Then there's the time period of the first few months of the pandemic, when the US actually made it harder for the commercial testing companies to get their tests approved, the CDC had this very low volume test that didn't work at first, and they weren't letting people test. The travel ban came too late, and it was too narrow to do anything. Then, after the first few months, eventually we figured out about masks, and that leadership is important.

**So you're disappointed, but are you *surprised*?**

I'm surprised at the US situation because the smartest people on epidemiology in the world, by a lot, are at the CDC. I would have expected them to do better. You would expect the CDC to be the most visible, not the White House or even Anthony Fauci. But they haven't been the face of the epidemic. They are trained to communicate and not try to panic people but get people to take things seriously. They have basically been muzzled since the beginning. We called the CDC, but they told us we had to talk to the White House a bunch of times.

Now they say, “Look, we’re doing a great job on testing, we don’t want to talk to you.” Even the simplest things, which would greatly improve this system, they feel would be admitting there is some imperfection and so they are not interested.

**Do you think it’s the agencies that fell down or just the leadership at the top, the White House?**

We can do the postmortem at some point. We still have a pandemic going on, and we should focus on that. The White House didn’t allow the CDC to do its job after March. There was a window where they were engaged, but then the White House didn’t let them do that. So the variance between the US and other countries isn’t that first period, it’s the subsequent period where the messages—the opening up, the leadership on masks, those things—are not the CDC’s fault. They said not to open back up; they said that leadership has to be a model of face mask usage. I think they have done a good job since April, but we haven’t had the benefit of it.

**At this point, are you optimistic?**

Yes. You have to admit there’s been trillions of dollars of economic damage done and a lot of debts, but the innovation pipeline on scaling up diagnostics, on new therapeutics, on vaccines is actually quite impressive. And that makes me feel like, for the rich world, we should largely be able to end this thing by the end of 2021, and for the world at large by the end of 2022. That is only because of the scale of the innovation that’s taking place. Now whenever we get this done, we will have lost many years in malaria and polio and HIV and the indebtedness of countries of all sizes and instability. It’ll take you years beyond that before you’d even get back to where you were at the start of 2020. It’s not World War I or

World War II, but it is in that order of magnitude as a negative shock to the system.

**In March it was unimaginable that you'd be giving us that timeline and saying it's great.**

Well it's because of innovation that you don't have to contemplate an even sadder statement, which is this thing will be raging for five years until natural immunity is our only hope.

**Let's talk vaccines, which your foundation is investing in. Is there anything that's shaping up relatively quickly that could be safe and effective?**

Before the epidemic came, we saw huge potential in the RNA vaccines—Moderna, Pfizer/BioNTech, and CureVac. Right now, because of the way you manufacture them, and the difficulty of scaling up, they are more likely—if they are helpful—to help in the rich countries. They won't be the low-cost, scalable solution for the world at large. There you'd look more at AstraZeneca or Johnson & Johnson. This disease, from both the animal data and the phase 1 data, seems to be very vaccine preventable. There are questions still. It will take us a while to figure out the duration [of protection], and the efficacy in elderly, although we think that's going to be quite good. Are there any side effects, which you really have to get out in those large phase 3 groups and even after that through lots of monitoring to see if there are any autoimmune diseases or conditions that the vaccine could interact with in a deleterious fashion.

**Are you concerned that in our rush to get a vaccine we are going to approve something that isn't safe and effective?**

Yeah. In China and Russia they are moving full speed ahead. I bet there'll be some vaccines that will get out to lots of patients without the full regulatory review somewhere in the world. We probably need three or four months, no matter what,

of phase 3 data, just to look for side effects. The FDA, to their credit, at least so far, is sticking to requiring proof of efficacy. So far they have behaved very professionally despite the political pressure. There may be pressure, but people are saying no, make sure that that's not allowed. The irony is that this is a president who is a vaccine skeptic. Every meeting I have with him he is like, "Hey, I don't know about vaccines, and you have to meet with this guy Robert Kennedy Jr. who hates vaccines and spreads crazy stuff about them."

**Wasn't Kennedy Jr. talking about you using vaccines to implant chips into people?**

Yeah, you're right. He, Roger Stone, Laura Ingraham. They do it in this kind of way: "I've heard lots of people say X, Y, Z." That's kind of Trumpish plausible deniability. Anyway, there was a meeting where Francis Collins, Tony Fauci, and I had to [attend], and they had no data about anything. When we would say, "But wait a minute, that's not real data," they'd say, "Look, Trump told you you have to sit and listen, so just shut up and listen anyway." So it's a bit ironic that the president is now trying to have some benefit from a vaccine.

**What goes through your head when you're in a meeting hearing misinformation, and the President of the United States wants you to keep your mouth shut?**

That was a bit strange. I haven't met directly with the president since March of 2018. I made it clear I'm glad to talk to him about the epidemic anytime. And I have talked to Debbie Birx, I've talked to Pence, I've talked to Mnuchin, Pompeo, particularly on the issue of, Is the US showing up in terms of providing money to procure the vaccine for the developing countries? There have been lots of meetings, but we haven't been able to get the US to show up. It's very important to be able to tell the vaccine companies to build extra factories for the billions of doses, that there is

procurement money to buy those for the marginal cost. So in this supplemental bill, I'm calling everyone I can to get 4 billion through GAVI for vaccines and 4 billion through a global fund for therapeutics. That's less than 1 percent to the bill, but in terms of saving lives and getting us back to normal, that under 1 percent is by far the most important thing if we can get it in there.

https://arstechnica.com/?p=1697546

---

# Appeals court rules 10¢-a-page charge for court documents is too high

Aurich Lawson / Getty Images

## reader comments

40 with 38 posters participating, including story author

## Share this story

A federal appeals court has ruled that the federal judiciary has been overcharging thousands of users for access to public court records. PACER, short for Public Access to Court Electronic Records, is an online system that allows members of the public (including Ars Technica reporters) to download documents related to almost any federal court case. For PDF documents, the site charges 10 cents per page—a figure far above the costs of running the system.

In 2016, three nonprofit organizations sued the judiciary itself over the issue. The class action lawsuit, filed on behalf of almost everyone who pays PACER fees, argued that the courts were only allowed to charge enough to offset the costs of running PACER. Over the last 15 years, as storage and bandwidth costs fell, the courts actually raised PACER fees from 7 cents to 10 cents. The courts used the extra profits to pay for other projects, like installing speakers and displays in courtrooms.

The plaintiffs argued that the courts were only allowed to charge the marginal cost of running PACER—which would be a fraction of the current fees. The government claimed that the law gave the courts broad discretion to decide how much to charge and how to use the money. In a 2018 ruling, a trial court judge charted a middle course. She ruled that some uses of PACER fees had exceeded Congress's mandates. But she didn't go as far as plaintiffs wanted by limiting spending to the operation of the PACER system itself.

## The Federal Circuit gets its say

A three-judge panel of appellate judges heard oral arguments on the case in February. Those judges seemed a bit incredulous at the judiciary's argument. Judge Raymond Clevenger seemed to be a leading skeptic:

> *Clevenger asked incredulously whether it would be legal for PACER fees to be used to replace "the curtains at the Supreme Court" and to buy "the Chief Justice's new chair."*
>
> *"We're redecorating all judges' offices with gold plates," he said sarcastically. Under the judiciary's theory, he said, "there's absolutely no remedy" for this kind of illegal spending.*

Thursday's ruling was written by Judge Todd Hughes and

supported by the other two judges on the case. It confirms that the judges weren't buying what the government's lawyers were selling. The government had argued that the judiciary shouldn't hear the case at all because the plaintiffs lacked standing. The Federal Circuit Appeals Court flatly rejected that argument, finding that if the government overcharged PACER users, then they have a right to sue to get their money back.

The appeals court upheld the lower court's finding that some of the judiciary's spending—including a pilot program for using PACER software for state courts in Mississippi, a system for communicating with jurors, and efforts to upgrade audiovisual technology in courtrooms—shouldn't have been done with PACER funds. The government will likely have to issue refunds to PACER users to cover these misuses of PACER funds.

At the same time, the appellate court agreed with the trial judge that the plaintiff's theory—that PACER fees could only be spent on costs directly related to serving PACER users—was too restrictive. According to the three-judge panel, the judiciary has latitude to spend PACER fees on any project that's somehow related to distributing electronic docket information to the general public.

## CM/ECF in the balance

One of the big open questions here is about CM/ECF, the electronic system that plaintiffs and defendants use to submit documents to the judiciary. In a sense, CM/ECF and PACER are two sides of the same system, since documents uploaded to CM/ECF become available for download by PACER users. However, CM/ECF isn't available to the general public. And the courts would likely need such an electronic docketing system even if PACER didn't exist.

So we can expect the plaintiffs in the case to argue that CM/ECF should be paid for some other way—perhaps by charging

higher fees to litigants or by having Congress appropriate money from general tax revenues. They'll argue that CM/ECF is only available to parties and their attorneys, not the general public, and hence isn't a system for public access to court records.

The government, in contrast, is likely to argue that PACER and CM/ECF constitute a single integrated system, so it's appropriate to use PACER fees to fund CM/ECF.

The Federal Circuit Appeals Court opted not to resolve that question in Thursday's ruling. Instead, it sent the case back down to the trial court, where the judge will have to sort out exactly which uses of PACER fees pass the standards laid out by the appeals court.

https://arstechnica.com/?p=1697574

---

# New Jersey prosecutors drop charges over tweeting a cop's photo [Updated]

Kevin Alfaro / Aurich Lawson / Getty Images

## reader comments

201 with 101 posters participating, including story author

## Share this story

A New Jersey man is facing felony charges for a tweet seeking to identify a police officer. Four others are facing felony charges for retweeting the tweet, the Washington Post reports.

Kevin Alfaro was attending a Black Lives Matter protest in the New York suburb of Nutley, New Jersey in June. He snapped a photo of a masked police officer and tweeted, “If anyone knows who this bitch is throw his info under this tweet.”

In a GoFundMe campaign to cover his legal fees, Alfaro explained that he had been “physically threatened” by counter-protesters during the Black Lives Matter demonstration. He was trying to identify an officer who seemed to be friends with one of the counter-protestors, who Alvarao considered a “blatant racist.”

Initially, Alfaro’s tweet got little attention. It was retweeted only a handful of times and was eventually deleted. But it caught the attention of the Nutley Police Department. In Mid-July, Alfaro and others were charged with cyber-harassment. That’s a fourth-degree felony that carries penalties of up to 18 months in prison.

“I simply retweeted because I feel that just as with anyone we should hold our officers accountable,” wrote Georgana Sziszak, one of the defendants, in a GoFundMe campaign to cover her legal fees. “I never heard of retweeting a tweet being a crime let alone a felony.”

The complaint against Sziszak claims that the tweet caused the officer to “fear that harm will come to himself, family, and property.”

“As a 20 year old that simply retweeted a tweet to help my friend, I am now at risk of giving up my career, serving time, and having a record,” Sziszak wrote.

## Strong defenses available

Sziszak's retweet is "clearly protected by the First Amendment," said Alan Peyrouton, Sziszak's attorney, in an interview with Ars. "I've never had a case like this."

Peyrouton points out that there's caselaw in the Third Circuit—the federal judicial circuit that encompasses New Jersey—protecting the right to photograph public officials. He also points out that there are legitimate, non-harassing reasons to seek identifying information about a police officer. For example, Alfaro could have been interested in filing a formal complaint about the officer's conduct.

And Eric Goldman, an Internet law scholar at Santa Clara University, tells Ars that people who merely retweeted the original tweet are likely to have another legal defense available: Section 230 of the Communications Decency Act.

Section 230 is most often invoked by online service providers like Twitter to shield them against liability for user content. But Section 230 says that "no provider *or user*" of an online service can be held responsible for another person's content. If Sziszak merely retweeted Alfaro's post, she should enjoy the same immunity Twitter does.

https://arstechnica.com/?p=1697450

---

# Mass hijacking spree takes over subreddits to promote

# Donald Trump

## reader comments

77 with 65 posters participating, including story author

## Share this story

Dozens of discussion groups on Reddit—including those dedicated to the National Football League, the San Francisco 49ers, and the Gorillaz—were hit in a Friday morning mass takeover spree that used the subreddits to spread messages promoting President Trump.

The hijacked accounts had tens of millions of combined members. The 148,000-member subreddit Supernatural, dedicated to the TV show by the same name, was emblazoned with pro-Trump images and slogans. Reddit personnel have since restored the moderator account to its rightful owner. The image above is how the subreddit appeared when the takeover was still active. The takeovers came five weeks after Reddit banned /r/The_Donald, a leading forum for fans of the president, and hundreds of other unrelated subreddits for violating recently rewritten content rules.

Reddit personnel published this post captioned, “Ongoing incident with compromised mod accounts.” Reddit personnel then warned that moderator accounts were being compromised and used to vandalize subreddits. It asked moderators of affected subreddits to report them in responses. At the time this post when live, the list of reported subreddits included:

A larger list of subreddits reported as compromised is available at the incident report linked above.

# Reddit investigates

Reddit officials issued the following statement: “An investigation is underway related to a series of vandalized communities. It appears the source of the attacks were compromised moderator accounts. We are working to lock down those accounts and restore impacted communities.”

The statement didn’t answer a question seeking the total number of affected subreddits. The company also didn’t respond to my inquiry on how those responsible for the hijackings carried them out. In an update published after this Ars article went live, Reddit personnel said that none of the compromised accounts were protected by two-factor authentication. Without the benefit of 2FA, compromised passwords that are reused on Reddit would be enough for attackers to access the accounts.

Several readers reported that they were receiving internal server errors when trying to enroll their accounts in 2FA. Others said after enabling 2FA they were no longer able to see notifications or start private conversations. Other users, meanwhile, complained that 2FA blocks or interferes or with their ability to use scripts that they use to manage subreddits.

Tweets from a Twitter account that appeared to also be compromised took responsibility for the mass Reddit account takeovers. The person controlling the Twitter account claimed the compromised accounts used weak passwords. The claims couldn’t immediately be confirmed. Twitter later suspended the account, and company representatives didn’t immediately return an email asking why.

At the time this post went live, most or all of the affected accounts appeared to have been either restored and reverted back to their previous condition or banned for terms of service violations.

Friday’s incident comes three weeks after hackers hijacked the accounts of celebrities, executives, and celebrities and tweeted links to a bitcoin scam to tens of millions of followers. Twitter has since said it lost control of its internal systems after an employee was tricked by a phone-based phishing attack. Prosecutors have charged a 17-year-old with being the mastermind behind the stunt. https://arstechnica.com/?p=1697514

---

# Trump declares TikTok, WeChat “national emergency,” preps bans

Enlarge / If the Trump administration has its way, these logos will be scarce inside the US in a few weeks.

### reader comments

260 with 105 posters participating

### Share this story

## Trade War! USA v. China

View more stories

The White House’s campaign against the China-based developers of popular apps escalated dramatically in the last day, as President Donald Trump declared both TikTok and WeChat to be

national emergencies and said the administration will ban or curtail their operations in September.

Trump late Thursday signed a pair of very similar executive orders "addressing the threat" allegedly posed by TikTok and WeChat.

"The spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States," both orders read. "The United States must take aggressive action against the owners" of the apps "to protect our national security."

## Why?

The White House explained its "national security" concerns about the apps and their parent firms in a pair of highly similar letters to congressional leaders.

TikTok "automatically captures vast swaths of information from its users," the TikTok letter reads, continuing:

> *This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage. TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities. TikTok may also be used for disinformation campaigns that benefit the Chinese Communist Party.*

WeChat does all that, too, the other letter alleges, and it also "captures the personal and proprietary information of Chinese nationals visiting the United States, thereby allowing

the Chinese Communist Party a mechanism for keeping tabs on Chinese citizens who may be enjoying the benefits of a free society for the first time in their lives."

The political rhetoric in the orders makes it clear that in addition to concern about Americans' user data potentially being sent to and digested by a foreign government, the orders are also part of the ever-escalating trade tensions between the Trump administration and China that has led to bans on equipment from Huawei and ZTE and increased tariffs on imported goods, among other actions.

## What does "aggressive action" look like?

The exact parameters of the orders are vague and unspecific, but neither explicitly bans the use of WeChat or TikTok in the US. Nor do the orders technically prohibit the developers' respective parent companies Tencent and ByteDance from operating in the United States.

What the orders do ban, however, are "transactions" related to ByteDance or WeChat—but not, apparently, the rest of Tencent. Those transactions are not clearly identified in either order, which instead say that the Secretary of Commerce (currently Wilbur Ross) has 45 days to "identify the transactions subject" to the order.

The order does not appear to conflict with Microsoft's plans to acquire TikTok, provided that the companies do indeed manage to get through talks and pull off a deal by September 15. However, the orders could theoretically prohibit distribution of the apps by the Apple App Store or Google Play, which would effectively keep them out of the hands (and off of the phones) of new users in the United States.

TikTok, like other social networks, makes money through both

in-app purchases and selling advertising. It is possible that either or both of those revenue streams could be cut off by the order, as selling anything to users or to businesses could be considered a kind of transaction.

WeChat is not widely used inside the United States. In China, however, it's basically the everything app. Where an American mobile user might cue up Uber, Amazon, GrubHub, Facebook Messenger, Venmo, and Apple or Google Pay to run through an hour's worth of chat and errands, a mobile user in China would do basically all of that and more through WeChat. All of those functions help generate revenue for WeChat, but it's not clear which would or would not be considered "transactions" for the administration's purposes.

## "Clean Network" purge

The orders are part of a new "Clean Network" initiative the State Department announced Wednesday. The initiative is nominally a "comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP)."

The Clean Network program, like the executive orders, is not particularly detailed, but its overall goal is clear from its five key "lines of effort," all of which aim to keep Chinese firms far away from US consumers, networks, and technologies.

The orders affecting WeChat and ByteDance both seem to stem from the "Clean Store" initiative "to remove untrusted applications from US mobile app stores." According to the State Department, apps from China "threaten our privacy, proliferate viruses, and spread propaganda and disinformation."

Plenty of homegrown US apps, such as Facebook and Twitter, have also been used to spread disinformation, sometimes on

behalf of foreign actors, but the “Clean Network” initiative does not address those concerns.

## Can they even do that, though?

Maybe?

US regulators have been probing TikTok since November, when the Committee on Foreign Investment in the United States, or the CFIUS, launched a review of the app. The CFIUS, a multi-agency committee headed by the Treasury Department, reviews transactions in which a foreign buyer acquires a US firm for potential national security concerns. TikTok formed when ByteDance bought a US service in 2017 and then rebranded and relaunched it under the TikTok name. The CFIUS did not review the Musical.ly deal at the time, but is now doing so retroactively.

The executive order against TikTok, however, does not cite the CFIUS review, and the CFIUS has not issued a public report or statement about the investigation. WeChat has not been under investigation by the CFIUS.

The orders were issued under the International Emergency Economic Powers Act (PDF), which allows the executive to issue orders regulating international commerce “to deal with any unusual and extraordinary threat.”

Because the orders are so vague, it’s hard to tell if they are justified under that legal basis. However the details may shake out, though, it is all but guaranteed that any attempt at enforcement will face immediate legal challenges.

“We are shocked by the recent executive order,” TikTok said in a statement. “For nearly a year, we have sought to engage with the US government in good faith,” the company added. “There has been, and continues to be, no due process or adherence to the law… This executive order risks undermining global

businesses’ trust in the United States’ commitment to the rule of law.

“We will pursue all remedies available to us in order to ensure that the rule of law is not discarded and that our company and our users are treated fairly—if not by the Administration, then by the US courts.”

https://arstechnica.com/?p=1697440

---

# HS suspends teen who tweeted photo of hallway packed with maskless students

Enlarge / Photo from North Paulding High School, tweeted by student Hannah Watters on Tuesday.

## reader comments

334 with 164 posters participating

## Share this story

A 15-year-old high school student who posted a viral photo of a crowded school hallway says the school suspended her for five days for allegedly violating a social-media policy. But the school has since backed down and lifted the suspension.

Hannah Watters, a student at North Paulding High School in Dallas, Georgia, posted a photo to Twitter on Tuesday, noting

the “jammed” hallways and “10 percent mask rate.” Her tweet received 1,800 retweets and 4,500 likes. She also posted a 10-second video of a hallway at the 2,000-student school and says she was suspended around noon the next day.

> *This is what it looks like even with split dismissal. pic.twitter.com/erCA2lhOUb*
>
> *— hannah (@ihateiceman) August 4, 2020*

“The policies I broke stated that I used my phone in the hallway without permission, used my phone for social media, and posting pictures of minors without consent,” Watters said, according to a BuzzFeed article. Watters called her actions “good and necessary trouble”—an apparent reference to a John Lewis quote—saying she is worried about the safety of students, faculty, and staff as the school reopens despite the ongoing coronavirus pandemic.

Her mother, Lynne Watters, said “the family is challenging the suspension,” according to the Atlanta Journal-Constitution. “Cell phone use is allowed in between classes and the sophomore waited until after regular school hours to post to social media, her mother said in a text message. ‘I feel they are selectively enforcing the rule in question,’ she wrote, adding that Hannah has never been in trouble at school.”

The newspaper article said one other student was suspended from the school for the same reason but didn’t name the other student. We contacted the school district today and will update this article if we get a response.

Watters’ appeal was apparently successful. “This morning my school called and they have deleted my suspension,” Hannah Watters tweeted this morning. “To everyone supporting me, I can’t thank you enough.”

State Schools Superintendent Richard Woods said in a statement

today that “discipline decisions are constitutionally the purview of local boards of education,” but he encouraged “districts and schools to operate with transparency, and to ensure that students and staff are not penalized for expressing their concerns,” according to the Journal-Constitution article. The newspaper also quoted Dr. Harry Heiman, clinical associate professor at Georgia State University’s School of Public Health, as saying that the hallway photo showed “exactly the kind of situation that school planning should ensure doesn’t happen.”

“It’s not a question of if that’s going to cause spread of the pandemic. It’s only a question of how quickly and to how many people,” Heiman said. Some members of the school football team had already tested positive for COVID-19 before the school reopened.

## District: Photo looks bad but is missing “context”

In a leaked audio recording, North Paulding High School Principal Gabe Carmona was heard warning students of “consequences” for posting photos or video “on social media that is negative in our light without permission.”

Paulding County School District Superintendent Brian Otott wrote a message about one of the viral photos to parents Tuesday night, saying that “some in the news media and some individuals on social media are taking this photo and using it without context to criticize our school reopening efforts.” Class changes are difficult, and the school district is “continuing to work… to find practicable ways to further limit students from congregating,” but “students are in this hallway environment for just a brief period as they move to their next class,” he wrote.

Otott admitted that “the photo does not *look* good,” but he

called it “unfortunate that in this day and age of instant communication these types of issues can escalate so quickly without sufficient context.” While many students were shown without masks, he wrote that “wearing a mask is a personal choice and there is no practical way to enforce a mandate to wear them.” Otott’s note to parents was published by TMZ.

Otott’s note also said that during this first week of school, students are going in person from Monday to Wednesday and “learning remotely on Thursday and Friday so that all of our schools can step back and assess how things are going so far.” The Thursday/Friday closure means that Watters did not miss a full day of in-person instruction.

Georgia Governor Brian Kemp on July 15 issued an executive order stating that cities and towns cannot impose mask-wearing requirements, and he sued Atlanta in an attempt to overturn the city’s mask mandate. Despite that, Atlanta is imposing a mask mandate in schools as well. Atlanta and the governor are in settlement talks.

https://arstechnica.com/?p=1697456