Trump spreads #FireFauci hashtag on Twitter as pandemic continues



Enlarge / US President Donald Trump and Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, hold a press briefing with members of the White House Coronavirus Task Force on April 5, 2020, in Washington, DC.

reader comments

342 with 137 posters participating

Share this story

President Donald Trump yesterday retweeted a Republican politician’s call to fire Dr. Anthony Fauci from his post as director of the National Institute of Allergy and Infectious

Diseases.

Trump's decision to spread the anti-Fauci tweet came hours after Fauci, in an interview with CNN, said it's "obvious" that the United States could have saved lives by imposing social-distancing measures in February as health experts recommended.

DeAnna Lorraine, a Republican who failed in a primary bid for House Speaker Nancy Pelosi's congressional seat in California's 12th district last month, wrote yesterday that it's "Time to #FireFauci" in a tweet criticizing Fauci for his CNN interview. Less than an hour later, Trump posted a quote-retweet of Lorraine's #FireFauci call. "Sorry Fake News, it's all on tape. I banned China long before people spoke up," Trump wrote. (Trump was referring to a travel ban.)

> *Sorry Fake News, it's all on tape. I banned China long before people spoke up. Thank you @OANN https://t.co/d40JQkUZg5*
>
> *— Donald J. Trump (@realDonaldTrump) April 12, 2020*

Despite Trump's #FireFauci retweet, White House spokesperson Hogan Gidley said today that "This media chatter is ridiculous—President Trump is not firing Dr. Fauci. Dr. Fauci has been and remains a trusted advisor to President Trump," according to The Wall Street Journal.

Fauci: Earlier action could have saved lives

Fauci appeared on CNN yesterday afternoon and was asked about a New York Times report that said the following:

> *By the third week in February, the administration's top public health experts concluded they should recommend to Mr. Trump a new approach that would include warning the American*

> *people of the risks and urging steps like social distancing and staying home from work. But the White House focused instead on messaging and crucial additional weeks went by before their views were reluctantly accepted by the president—time when the virus spread largely unimpeded.*

CNN's Jake Tapper asked Fauci if lives could have been saved if social-distancing and stay-at-home measures were implemented in the third week of February instead of mid-March. This was Fauci's response:

> *It's the what would have, what could have, it's very difficult to go back and say that. I mean, obviously, you could logically say that if you had a process that was ongoing and you started mitigation earlier, you could have saved lives. Obviously, no one is going to deny that. But what goes into those kinds of decisions is complicated. But you're right, obviously if we had right from the very beginning shut everything down, it may have been a little bit different. But there was a lot of pushback about shutting things down back then.*

In another tweet, Trump claimed the New York Times article was "fake news."

Warnings in late February

Lorraine's tweet criticized Fauci for "saying that had Trump listened to the medical experts earlier he could've saved more lives," when Fauci himself "was telling people on February 29th that there was nothing to worry about and it posed no threat to the US public at large."

Lorraine was apparently referring to a February 29 *Today Show* interview in which Fauci said, "right now, at this moment, there is no need to change anything that you're doing on a day-by-day basis. Right now, the risk is still low, but this

could change."

Fauci also said in that interview that the US was in the beginning stages of community spread of the coronavirus, making it more difficult to track its spread. "When you start to see community spread, this could change and force you to become much more attentive to doing things that would protect you from spread," Fauci said.

A week before the *Today* interview, Fauci and other government health experts on the White House coronavirus task force met and "concluded they would soon need to move toward aggressive social distancing, even at the risk of severe disruption to the nation's economy and the daily lives of millions of Americans," according to the New York Times story. The question they were facing was not whether to take such measures, but when to take them.

Fauci walks fine line with Trump

Fauci, a renowned figure in public health who played a major role in the fight against HIV/AIDS, was appointed to his position in November 1984.

Last month, Science Magazine asked Fauci how he has avoided getting fired. "Well, that's pretty interesting because to [Trump's] credit, even though we disagree on some things, he listens," Fauci said in response. "He goes his own way. He has his own style. But on substantive issues, he does listen to what I say." Fauci has had to correct some of Trump's false statements but tries to do so in a tactful way. "I can't jump in front of the microphone and push him down," Fauci said.

Fauci's willingness to contradict Trump has angered Republicans such as former congressman Ron Paul, who last week called for his firing. "People have to quit listening to him," Paul said of Fauci, calling him a "fraud."

Although Fauci isn’t a political appointee, he’s not necessarily immune to a political ouster. “By and large, most of the civil servants the president has sought to purge from the ranks lack much in the way of due process rights,” national-security lawyer Bradley Moss was quoted as saying in a recent Hill article about Trump firing inspectors general at multiple federal agencies.

Trump could take an indirect approach by pressuring HHS Secretary Alex Azar to fire Fauci. Azar was nominated to his position by Trump in 2017 but has reportedly clashed with the president over the coronavirus response. Trump accused Azar of being alarmist about the potential of a pandemic on January 30, The New York Times report said. Azar was originally in charge of the White House’s coronavirus task force and is still technically its chairman, but Trump put Vice President Mike Pence in charge of the coronavirus response in late February.

Even if Trump doesn’t try to push Fauci out of the government completely, the president could sideline him from the task force and press briefings.

“Despite his critics, Dr. Fauci—through White House briefings and regular television interviews—has become a popular figure in the country,” The Wall Street Journal wrote today in an article about Trump’s retweet. “A Quinnipiac poll last week put [Fauci’s] approval rating at 78 percent for handling of the crisis, versus the 46 percent approval rating for the president.”

https://arstechnica.com/?p=1667950

IBM scrambles to find or train more COBOL programmers to help states



Enlarge / Stock photo shows computing systems from the COBOL era.
Lambert/Archive Photos

reader comments

185 with 116 posters participating

Share this story

The COBOL programming language was created in 1959 and has been widely seen as obsolete for decades. Yet there are still

a fair number of software systems based on the language. The economic stresses of the coronavirus pandemic have created a surge in demand for COBOL programmers. Last week, for example, the governor of New Jersey put out a call for COBOL programmers to help fix problems with the software that runs the state's unemployment insurance system.

A new initiative from IBM seeks to connect states with experienced COBOL programmers—and to train a new generation of them.

"In the midst of the COVID-19 global pandemic, our clients are facing unprecedented circumstances," an IBM press release says. Some states "are in need of additional programming skills to make changes to COBOL—a language that has been widely reported to have an estimated 220 billion lines of code being actively used today."

A new online forum, co-sponsored by the Open Mainframe Project, aims to connect COBOL programmers to people wanting to hire them. Several hundred COBOL programmers—some with decades of experience, others just learning the language—have submitted their information to the site.

A second forum is "being actively monitored by experienced COBOL programmers providing free advice and expertise during the crisis. This tool will allow all levels of programmers to manage issues, learn new techniques, and expedite solutions needed as programmers alter this critical code."

IBM is also working on a free COBOL training course. The company has posted some material to Github, though it falls short of a full COBOL training course. IBM's announcement says that the material "will be made into a self-service video course with hands-on labs and tutorials available via Coursera and other learning platforms next month."

It may not be feasible to train new COBOL programmers in time for them to help with urgent problems like New Jersey's creaky

unemployment insurance system. But it doesn’t look like COBOL will be going away any time soon, and today’s most experienced COBOL programmers aren’t getting any younger.

https://arstechnica.com/?p=1667866

Nine Amazon workers describe the daily risks they face in the pandemic



Enlarge / An Amazon Prime-branded delivery van and driver.

reader comments

46 with 31 posters participating

Share this story

As the novel coronavirus pandemic sweeps the globe, an otherwise marginalized class of workers is suddenly in the spotlight. Often undervalued and poorly paid, they are grocery store clerks, sanitation workers, medical professionals, and other employees who can’t stay home—even when the nation is on lockdown. In the United States, hundreds of thousandsof these so-called essential workers are employed by or contract for Amazon, whose delivery network has emerged as a vital service for millions of Americans stuck inside their homes.

Wired spoke with nine people working for Amazon during the Covid-19 crisis over the past two weeks and is publishing their accounts of being on the job, in their own words. They work in Amazon fulfillment centers, deliver packages and groceries, and stock food in Amazon cafeterias. Some are employed by Amazon directly, while others are contractors. Each of them say they are terrified for their health and that of their families, and many believe Amazon isn’t doing enough to ensure their safety. While the company has often framed its frontline workers as heroes, the people WIRED spoke with say they didn’t sign up for this level of risk.

Covid-19 has now spread to at least 50 Amazon facilities in the US, out of a total of more than 500, according to *The New York Times*. The outbreaks have led to employee protests in Detroit, New York City, and Chicago, where workers said Amazon was slow to notify them about infections and failed to conduct adequate cleaning. At Amazon-owned Whole Foods, staff staged a nationwide demonstration citing similar safety concerns and calling for free coronavirus testing for all employees. And more than 5,000 Amazon workers have signed a petition asking for additional benefits given the health crisis, including hazard pay and for the company to shut down any facility where a worker tests positive so it can be properly cleaned.

WIRED

Amazon’s practices have attracted the attention of lawmakers including senators Bernie Sanders, Cory Booker, Robert Menendez, and Sherrod Brown, who sent a letter to Amazon CEO Jeff Bezos last month demanding answers about the company’s workplace safety measures. “Any failure of Amazon to keep its workers safe does not just put their employees at risk, it puts the entire country at risk,” they wrote. On Wednesday, the Occupational Safety and Health Administration announced it was investigating an Amazon warehouse in Pennsylvania after workers there said their health wasn’t being protected. Workers at a warehouse in California filed similar complaints with state and county regulators the same day.

“Our employees are heroes fighting for their communities and helping people get critical items they need in this crisis. Like all businesses grappling with the ongoing Covid-19 pandemic, we are working hard to keep employees safe while serving communities and the most vulnerable,” an Amazon spokesperson said in a statement. “We have taken extreme measures to keep people safe, tripling down on deep cleaning, procuring safety supplies that are available, and changing processes to ensure those in our buildings are keeping safe distances.”

Amazon says it has made over 150 changes to help protect its workforce, including distributing face masks to all staff, instituting social-distancing protocols, staggering shift start times, and adding more space between workstations. The company is also checking whether employees have a fever when they show up for their shifts, though the practice won’t detect the significant number of Covid-19 cases that are asymptomatic. The Amazon spokesperson said it’s just “one of the many preventative measures Amazon is taking to support the health and safety of our customers and employees.”

In recent weeks, Amazon has raised wages for hourly workers and said it would let anyone concerned about coming into work to take unpaid time off through the end of April. After receiving criticism from lawmakers, it will also now allow anyone suspected of having Covid-19 or placed into quarantine to take two weeks of emergency paid sick leave. Prior to March 27, the company required that workers obtain a positive test result to use the benefit, but a nationwide testing shortage made that extremely difficult.

The following interviews have been condensed and edited for clarity.

Warehouse worker, early forties, Texas

My partner and I have both been working at Amazon for a few years. We're awesome at what we do. I love the job itself, but I don't like how the company handles people—almost like they're disposable.

Since the virus came, for the last couple of weeks, we've taken advantage of the unpaid—not paid—time off. This next upcoming paycheck, I think I will be paid for six hours of work. I'm staying home because my mom, she had a pacemaker put in not too long ago, and she lives with me. We don't want to go without money. In fact, I don't know how we're going to pay our bills this month. I'm down to about $200, and this stimulus check is probably not going to come for another month.

Amazon releases their own little news alerts, and one of them told us that we need to make sure we're cleaning our scanners. They told us to do it—the people who are also working on the floor, who are also responsible for getting a certain number of packages out every shift. This is what kills me: When we walk through the main front doors, we hit these turnstiles to

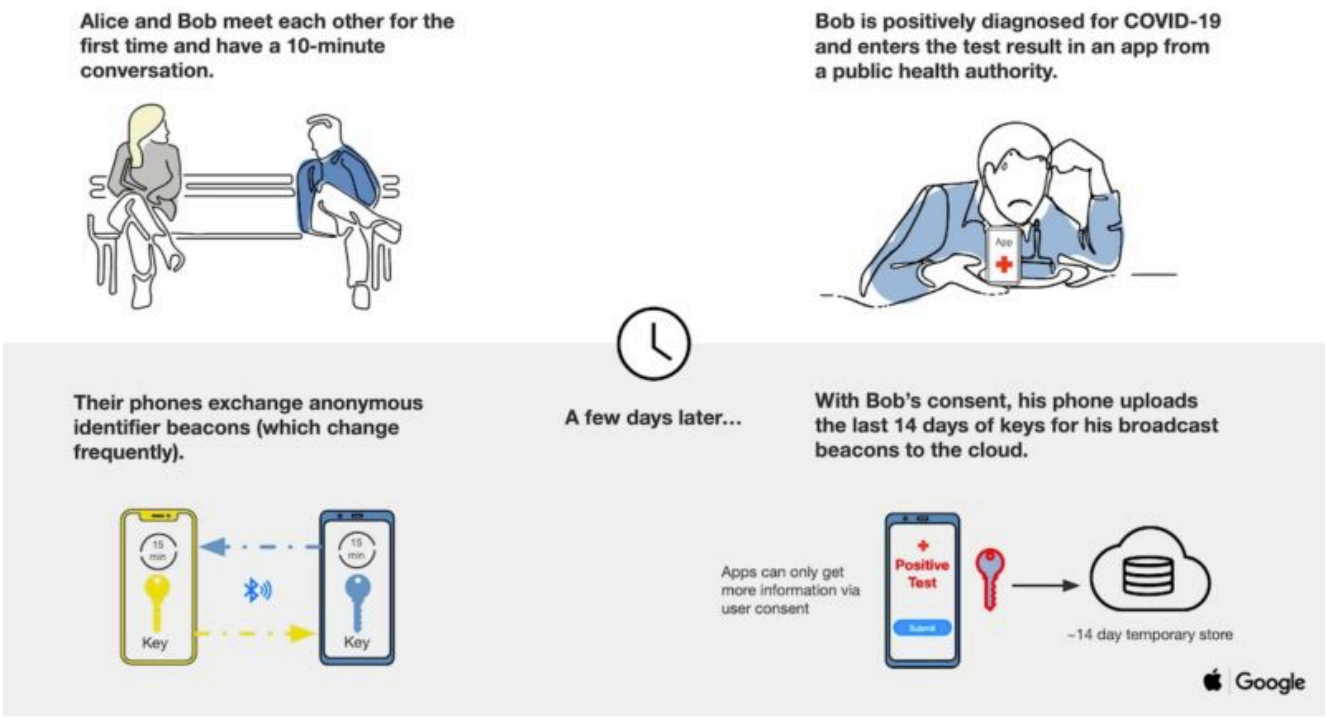
enter. Everyone has to touch them, and I have never, not one time in my life, seen anybody clean those things. I know that in my fulfillment center, we've got over 900 people who work there, and we have three entrances to choose from. All it's going to take is one infected person.

You've got people that are working for $15 an hour, that now have to be excited that they're making $17 an hour, going out there and basically putting their family at risk. If you're saying our job is so damn important, and that everybody else should stay home, yet we have to show up like soldiers, why not protect us?

The day this interview was conducted, Amazon notified the worker about a confirmed case of Covid-19 at their workplace.

https://arstechnica.com/?p=1667542

Apple and Google detail bold and ambitious plan to track COVID-19 at scale



reader comments

118 with 71 posters participating

Share this story

In a bold and ambitious collaboration, Apple and Google are developing a smartphone platform that tries to track the spread of the novel coronavirus at scale and at the same time preserve the privacy of iOS and Android users who opt in to it.

The cross-platform system will use the proximity capabilities built into Bluetooth Low Energy transmissions to track the physical contacts of participating phone users. If a user later tests positive for COVID-19, the disease caused by the coronavirus, she can choose to enter the result into a health department-approved app. The app will then contact all other participating phone users who have recently come within six or so feet of her.

The system, which Google and Apple described here and here respectively, applies a technological approach to what's known

as contact tracing, or the practice of figuring out everyone an infected individual has recently been in contact with. A recently published study by a group of Oxford researchers suggested that the novel coronavirus is too infectious for contact tracing to work well using traditional methods. The researchers proposed using smartphones, since they're nearly ubiquitous, don't rely on faulty memories of people who have been infected, and can track a nearly unlimited number of contacts of other participating users.

Mitigating the worst

But while mobile-based contact tracing may be more effective, it also poses a serious threat to individual privacy, since it opens the door to central databases that track the movements and social interactions of potentially millions, and possibly billions, of people. The platform Apple and Google are developing uses an innovative cryptographic scheme that aims to allow the contact tracing to work as scale without posing a risk to the privacy of those who opt into the system.

Privacy advocates—with at least one notable exception—mostly gave the system a qualified approval, saying that while the scheme removed some of the most immediate threats, it may still be open to abuse.

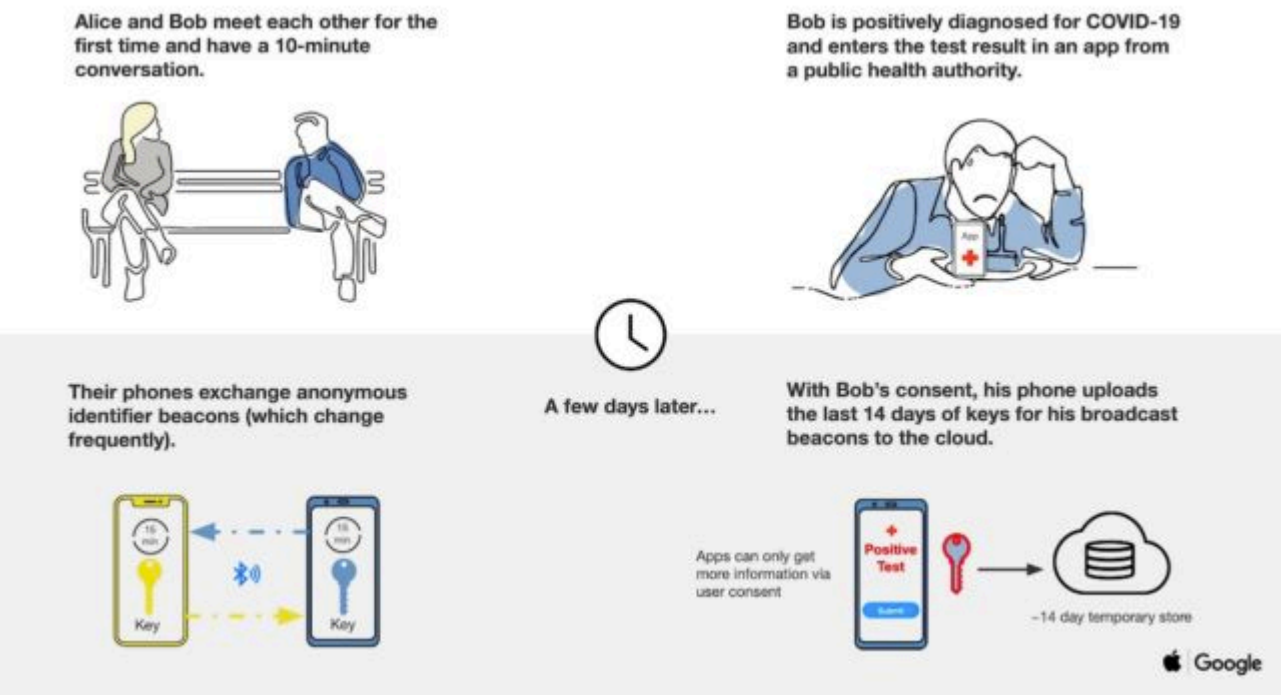
"To their credit, Apple and Google have announced an approach that appears to mitigate the worst privacy and centralization risks, but there is still room for improvement," Jennifer Granick, surveillance and cybersecurity counsel for the American Civil Liberties Union, wrote in a statement. "We will remain vigilant moving forward to make sure any contact tracing app remains voluntary and decentralized, and used only for public health purposes and only for the duration of this pandemic."

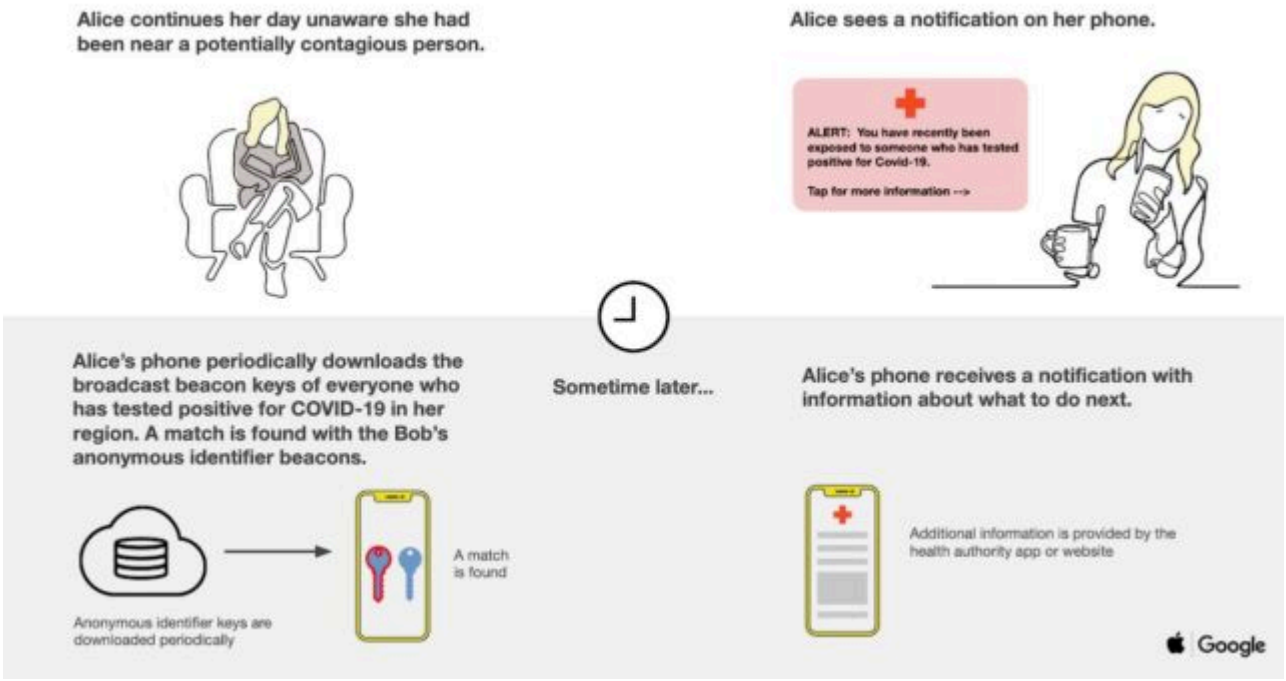
Unlike traditional contact tracing, the phone platform doesn't collect names, locations, or other identifying information.

Instead, when two or more users opting into the system come into physical contact, their phones use BLE to swap anonymous identifier beacons. The identifiers—which in technical jargon are known as rolling proximity identifiers—change roughly every 15 minutes to prevent wireless tracking of a device.

As the users move about and come into proximity with others, their phones continue to exchange these anonymous identifiers. Periodically, the users' devices will also download broadcast beacon identifiers of anyone who has tested positive for COVID-19 and has been in the same local region.

In the event someone reports to the system that she has tested positive, her phone will contact a central server and upload 14 days of her identifiers. Non-infected users download daily tracing keys, and because of the way each rolling proximity identifier is generated, end-user phones can recreate them indexed by time from just the daily tracing key for each day. The following two slides help illustrate at a high level how the system works.





Apple and Google are providing other assurances, including:

- Explicit user consent required
- Doesn't collect personally identifiable information or user location data
- List of people you've been in contact with never leaves your phone
- People who test positive are not identified to other users, Google or Apple
- Will only be used for contact tracing by public health authorities for COVID-19 pandemic management
- Doesn't matter if you have an Android phone or an iPhone—works across both

How it works (in theory)

Jon Callas, a cryptography expert and senior technology fellow at the ACLU, told me that the scheme is similar to the way raffle tickets work, with one party getting half of a paper ticket, the other party getting the other half, and—in theory at least—no one else being the wiser. When two phone users come into physical proximity, they BLE transmitters exchange tickets. Callas said that a similar COVID-19 tracking scheme

known as the Pan-European Privacy-Preserving Proximity Tracing appears to work roughly the same way.

“I keep a list of all the tickets I have,” he said. “If Alice tests positive, she releases her tickets and if ones that I have match, I know I had a contact with a positive person.” Callas went on to caution that ambiguities in the flow of both the Apple-Google platform and the Pan-European Privacy-Preserving Proximity Tracing leave open the possibility of abuse because it’s not yet clear which parties get access to which tickets.

“If Alice releases the tickets she sent *and* the ones she received, she’s outing the people who were near her,” he said.

Callas said he was involved in development of a third tracking scheme known as PACT, short for Private Automatic Contact Tracing. By contrast, he said, it has assurances that parties can only release sent tickets.

Begging to differ

Moxie Marlinspike, a hacker and developer who has both broken advanced crypto schemes and built them, was among the most vocal critics of the scheme as laid out. In a twitter thread that analyzed the way the APIs and cryptography interacted, he raised serious doubts about the plan.

“So first obvious caveat is that this is ‘private’ (or at least not worse than BTLE), *until* the moment you test positive,” he wrote in one tweet. “At that point all of your BTLE mac addrs [BLE MAC addresses] over the previous period become linkable. Why do they change to begin with? Because tracking is already a problem.”

> *So it takes BTLE privacy a ~step back. I don’t see why all of the existing beacon tracking tech wouldn’t incorporate this into their stacks.*

> *At that point adtech (at minimum) probably knows who you are, where you've been, and that you are covid+.*
>
> *— Moxie Marlinspike (@moxie)* ***April 10, 2020***

Marlinspike, who is the creator of the Signal encrypted messenger app and the CEO of of the the company that stewards it, said the next weakness is the amount of data that might have to be transmitted to user phones:

> *Second caveat is that it seems likely location data would have to be combined with what the device framework gives you.*
>
> *Published keys are 16 bytes, one for each day. If moderate numbers of smartphone users are infected in any given week, that's 100s of MBs for all phones to DL*
> *That seems untenable. So to be usable, published keys would likely need to be delivered in a more 'targeted' way, which probably means… location data.*

> *That seems untenable. So to be usable, published keys would likely need to be delivered in a more 'targeted' way, which probably means… location data.*
>
> *— Moxie Marlinspike (@moxie)* ***April 10, 2020***

Another possible weakness: trolls might frequent certain areas and then report a false infection, leading large numbers of people to think they may have been exposed. These kinds of malicious acts could be prevented by requiring test results to be digitally signed by a testing center, but details released on Friday, didn't address these concerns. A variation of falsifying positive results is relaying BLE IDs collected from a hospital or other targeted area.

Technologist and privacy advocate Ashkan Soltani provided additional privacy critiques in this Twitter thread:

> *In my opinion — these types of data are poor proxies for the ground truth we really seek: actual #COVID19 infection rates — which can only be truly known by widespread testing. If we had testing in place, it would make the need to pursue these privacy-invasive techniques moot*
>
> *— ashkan soltani (@ashk4n) April 10, 2020*

Soltani provided other useful details here and here.

Reading the specs

The cryptography behind the anonymous and ever-changing identifiers are laid out in this specification, which among other things assures that:

- The key schedule is fixed and defined by operating system components, preventing applications from including static or predictable information that could be used for tracking.
- A user's Rolling Proximity Identifiers cannot be correlated without having the Daily Tracing Key. This reduces the risk of privacy loss from advertising them.
- A server operator implementing this protocol does not learn who users have been in proximity with or users' location unless it also has the unlikely capability to scan advertisements from users who recently reported Diagnosis Keys.
- Without the release of the Daily Tracing Keys, it is not computationally feasible for an attacker to find a collision on a Rolling Proximity Identifier. This prevents a wide-range of replay and impersonation attacks.
- When reporting Diagnosis Keys, the correlation of Rolling Proximity Identifiers by others is limited to 24h periods due to the use of Daily Tracing Keys. The server must not retain metadata from clients

uploading Diagnosis Keys after including them into the aggregated list of Diagnosis Keys per day.

A separate Bluetooth specification, meanwhile, requires that:

- The Contact Tracing Bluetooth Specification does not require the user's location; any use of location is completely optional to the schema. In any case, the user must provide their explicit consent in order for their location to be optionally used.
- Rolling Proximity Identifiers change on average every 15 minutes, making it unlikely that user location can be tracked via bluetooth over time.
- Proximity identifiers obtained from other devices are processed exclusively on device.
- Users decide whether to contribute to contact tracing.
- If diagnosed with COVID-19, users consent to sharing Diagnosis Keys with the server.
- Users have transparency into their participation in contact tracing.

Coming to a phone near you

Apple and Google plan to release iOS and Android programming interfaces in May. They will be available public health authorities for developing apps running on one mobile operating system to work with apps running on the other. The official apps will then be available for download in Apple's App Store and Google Play. Eventually, the companies plan to introduce tracing functionality directly into the OSes. Presumably, users can activate the functionality with a setting change.

Besides the privacy risks, there are other potential flaws. The system could cause undue alarm if it sends a warning that someone was exposed, when in fact the other party was dwelling in the same apartment building but in separate units. Bluetooth is also prone to a variety of flaws that can

compromise its reliability and occasionally its security.

There are many important details that aren’t yet available and are crucial to understanding the privacy risks of the system Apple and Google are building. In normal times, it might be a given to advise people to opt out. Given the global health crisis presented by the ongoing pandemic, the call will be much harder to make this time around.

Post updated to correct the information uploaded from the phone of someone who tests positive.

https://arstechnica.com/?p=1667565

When school is online, the digital divide grows greater



Enlarge / A student studying on his laptop with two friends after classes were cancelled.
Phillipe Francois | Getty Images

reader comments

61 with 47 posters participating

Share this story

Like many students around the world, Nora Medina is adapting to online learning. But Medina, a high school senior in Quincy, Washington, who also takes classes at a local community college, faces an additional challenge: She doesn’t have reliable Internet service at home. She lives 7 miles outside of town where she says neither cable nor DSL Internet is available.

She can access the Internet on her phone, and her family has a wireless hotspot, but she says the service isn’t up to the task of doing homework online. “It’s hit and miss,” she says.

“Sometimes I can watch a video, but sometimes I can’t even refresh a page, or it will take minutes to load something on a page.”

Washington governor Jay Inslee this week said the state’s schools will be closed for the rest of the school year. Quincy High School is still planning how best to help students finish the year. But Medina’s classes at Big Bend Community College have shifted online. “I’m just going to hope the hot spot works and wish for the best for my final quarter,” she says. “If that doesn’t work, I’ll do my work from my car in the parking lot at the library to access their Wi-Fi.”

WIRED

Medina is one of millions of people in the US who lack reliable broadband Internet at home, either because they can’t afford it or because it simply isn’t available where they live. This digital divide has always left children and adults alike with fewer educational and economic opportunities. But with schools, libraries, and workplaces closed during the coronavirus pandemic, those without broadband are struggling to access schoolwork, job listings, unemployment benefit applications, and video chat services that others use to keep in touch with friends and family. For those on the wrong side of the digital divide, working from home isn’t an option.

The Federal Communications Commission says more than 650 broadband Internet providers, telephone companies, and trade associations have signed its Keep America Connected Pledge to not terminate Internet service over pandemic-related financial troubles, to waive late fees, and to allow free access to Wi-Fi services. Comcast said it would offer free access to its broadband service for low-income households, normally priced at $10 a month, for 60 days, and Charter said it would offer free Internet access for students for 60 days. But these offerings are available only in locations where those

companies already provide service.

It’s hard to gauge the extent of the problem. In a report last year, the FCC estimated that 21.3 million people had no access to broadband Internet service at the end of 2017. But the report, based on self-reported data from broadband providers, considers an entire census block to have service if a single broadband provider claims to offer service anywhere within the census block, even if most homes within the area can’t get service. Critics have long pointed out that this method likely underestimates the number of people without access to broadband.

A report published last year by Microsoft estimated that 162.8 million people in the US—about half the population—don’t use broadband Internet, whether because it’s unavailable where they live or they can’t or won’t pay for access. A survey commissioned by Microsoft and the National 4-H Council found that 20 percent of rural youth lack access to broadband at home, regardless of whether it’s available where they live.

How schools are coping

The digital divide creates a challenge for teachers and administrators who know some students can’t easily follow online lessons. Berkeley, California, schools closed in the middle of March, but the distinct didn’t begin online classes until Monday. In the interim, public schools superintendent Brent Stephens says officials had to work out how to accommodate special-needs students, adjust union contracts, and plan lessons for 16,000 students.

But, Stephens says, “equity has been a concern” too. He estimates that about 5 percent of the district’s students lack reliable Internet access at home, and about 30 percent need devices suitable for online learning. He says the district has distributed more than 2,000 Chromebooks to students and ordered wireless hotspots for students who don’t have reliable

Internet access at home, though it’s not clear when those hot spots will be available. In the meantime, the district is still considering how to get learning resources to students without Internet access.

Some schools are employing low-tech solutions. Bandon School District on Oregon’s southern coast plans to deliver and collect physical packets of learning materials and assignments to the 18 percent of students who superintendent Doug Ardiana says lacks Internet at home.

When Oregon governor Kate Brown closed schools on March 12, Bandon schools sent out “supplemental” learning assignments that didn’t need to be returned. Now, schools will be closed for the rest of the school year, and schools are supposed to offer distance-learning programs, including graded assignments.

To prepare students for those assignments, teachers are filming lessons that students can watch from home over the Internet. “It’s a whole new thing,” says Courtney Wehner, a third-grade teacher at Ocean Crest Elementary in Bandon. “I’m not used to hearing my voice recorded.”

For students who lack Internet access, the school will send packets of materials to their homes, either through the mail or with school bus drivers wearing protective gear. Students who can use them will get DVDs or thumb drives with the recorded lectures. Wehner says that includes all of her students. Others will have to depend on written materials.

Wehner says the parents of her students who lack broadband Internet will take pictures of completed assignments with their phones and send them to her for grading. Students in the district who can’t return assignments that way will send completed assignments back with bus drivers or the postal service, and someone at their school, also wearing protective gear, will scan the assignments and upload them to a server

that teachers can access from home. Teachers will review and correct the assignments and print them out, and the corrected assignments will go back to the students three days later.

A $20 billion fix for a $70 billion problem

The FCC has spent billions in recent years in the name of closing the digital divide. But that divide persists in part because the agency has repeatedly underestimated the scope of the problem, says FCC commissioner Jessica Rosenworcel. “How do we know we’re sending money to the right places?” she asks.

The Rural Digital Opportunity Fund, which replaced a previous initiative called the Connect America Fund, gives carriers money to build broadband in communities that lack access to connections of at least 10 megabits per second. It’s set to send $20.4 billion over 10 years to carriers to expand rural broadband access. But John Windhausen Jr., executive director of the Schools, Health & Libraries Broadband Coalition, says the Fiber Broadband Association estimated last year that it will cost $70 billion to bring fiber-optic networks to 90 percent of the US by 2025.

Beyond the pledges from carriers to not cut off service, the FCC has permitted libraries and public schools to offer public Wi-Fi while the buildings are closed without risking FCC funds, and has moved to dedicate a large chunk of spectrum for unlicensed Wi-Fi use instead of auctioning off licenses for it; advocates say that could make it easier to provide wireless broadband services in rural or low-income areas.

But critics say the FCC in recent years has impeded efforts to close the digital divide. Last year the FCC voted to auction off wireless spectrum that had been reserved for schools to the highest bidder, which Windhausen says will make it harder for schools, local governments, and nonprofits to use that

spectrum to create their own wireless services.

The FCC under Chairman Ajit Pai has resisted expansion of Lifeline, a 35-year-old program that subsidizes access to telecom service for low-income households. Lifeline has remained intact, though. In February 2019, a federal appeals court overturned Pai's attempt to limit broadband subsidies for tribal residents. Another Pai proposal that would have prevented poor people from buying Lifeline plans from network resellers was quietly scrapped after widespread condemnation. Pai pressed on in mid-2019 with a proposal to impose an overall cap on Universal Service spending, including Lifeline, but the plan hasn't been finalized.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1667547

COVID-19 tests are going unused due to hospital IT challenges



seksan Mongkhonkhamsao / Getty

reader comments

85 with 61 posters participating

Share this story

Testing is one of the most important tools for getting the coronavirus pandemic under control in the United States. More than 160,000 COVID-19 tests were performed in the US on Thursday, according to the COVID Tracking Project. But there's good reason to believe that there are still many people with the virus who have not been tested. More testing would help guide treatment and quarantine decisions and give government officials more data about the extent of the COVID-19 outbreak.

At the same time, a Nature investigation has revealed that a number of academic labs capable of performing COVID-19 tests are operating well below capacity. Nature's reporting suggests that incompatible IT systems are significant reasons for this

mismatch.

Many hospitals are used to working with large commercial labs that have the software necessary to interface with a hospital's electronic health records and billing systems. When an academic lab shows up with the capacity to run tests but not the infrastructure to interface with hospital systems, hospitals are often reluctant to do business with them.

Nature talked to Fyodor Urnov, who directs a genomics center at the University of California, Berkeley. The organization launched a testing service in late March and began pitching it to hospitals. His lab already has the Clinical Laboratory Improvement Amendments (CLIA) certification that is required to perform COVID-19 tests.

The tests would have been free to hospitals, funded by private philanthropists. But he still had trouble finding hospitals interested in working with him.

"The business of American medicine and the way it is organized is astonishingly unprepared for this," he told Nature. "I show up in a magic ship, with 20,000 free kits and CLIA and everything, and the major hospitals say: 'Go away, we cannot interface with you.'"

Urnov's lab wound up testing some patients outside the hospital system—including firefighters and homeless people. The non-profit group coordinating these tests doesn't have software compatible with the Berkeley testing service's software, but folks on both sides were willing to do manual data entry to accelerate the testing process.

Stacey Gabriel, a human geneticist at the Broad Institute of MIT and Harvard, told Nature that "our capacity is 2,000 tests a day, but we aren't doing that many. Yesterday was around 1,000."

Like Urnov's group, Gabriel's project has had to hustle to

find partners willing to be flexible enough to try a service that didn’t have the full infrastructure of a commercial testing lab. “It took about 2,000 phone calls and many e-mails, but we’re getting there,” Gabriel told Nature.

But she worries that logistical difficulties like this could prevent other labs from joining the testing effort.

https://arstechnica.com/?p=1667438

Lockdowns flatten the “economic curve,” too



Enlarge / The Oakland Municipal Auditorium in use as a temporary hospital during the 1918 flu pandemic.

reader comments

48 with 38 posters participating

Share this story

The lockdown measures being taken in response to the coronavirus pandemic are causing economic turmoil. Faced with this, President Donald Trump balked at the prospect of continuing those measures long-term, tweeting, “WE CANNOT LET THE CURE BE WORSE THAN THE PROBLEM ITSELF.”

But in reality, the best economic medicine may be the dreaded lockdown. A working paper by economists at the Federal Reserve and MIT digs into data from the 1918 flu pandemic and finds

that cities that reacted quickly and aggressively to the pandemic also had stronger economic growth after the crisis was over.

Looking backward

An armchair economist could happily predict the economic effects of a lockdown. Intuitively, freezing the economy of a city, state, or country by forcing everyone to stay home seems like it would be an unambiguously bad thing for that economy.

But “economic activity is also reduced in absence of such measures,” write economists Sergio Correia, Stephan Luck, and Emil Verner. Even without lockdown orders, people living through a pandemic have a tendency to stay home as much as possible and change their economic habits to minimize their chances of getting infected. So if a lockdown helps to bring an outbreak to heel more effectively, it could actually help to reduce economic damage.

The 1918 flu pandemic offers a potential insight into how city and state economies responded to different public health strategies. Peaking in the US in fall 1918, the pandemic is estimated to have killed around 600,000 people in the US and 50 million worldwide.

Just like in the current pandemic, there was a pretty wide range of responses to the outbreak. Some cities reacted promptly, implementing measures similar to those we’re seeing now—banning of mass gatherings, social distancing, and case isolation. Others were tardier. Correia and colleagues pulled together a range of sources of historical data to take a look at how different cities responded and how their economies fared afterward.

Causal spaghetti

The only thing that's really possible to do with this kind of historical data is look at correlations: whether cities that responded faster had, on average, better economic growth post-pandemic. The problem with correlations is that they can't show for sure whether the fast response boosted the economic growth or whether there's some other relationship between the two factors—like economically healthier cities having better public health infrastructure in the first place, or some third factor underlying both the response and the economic growth.

But by trying to think about what other explanations there could be and controlling for them in the analysis, it's possible to tease out which factors offer the most reasonable explanation for the data. That's what Correia and colleagues did. Places that responded faster in 1918 tended to be farther west, giving them a chance to witness what had happened as the pandemic hit first on the East Coast. But this also meant that places that shut down sooner had economies that were relatively agriculture-based.

This means that there were two simultaneous differences between groups of cities, making it difficult to tell which difference was more important—are any differences best explained by the western cities responding faster to the pandemic? Or did their more agriculture-based economies respond differently for other reasons?

To deal with this, the researchers made sure that their analysis accounted for the relative importance of agriculture compared to manufacturing in local economies. They also checked whether there were other systematic differences that they needed to control, like whether western regions had stronger average health infrastructure than eastern regions. And they accounted for the flu mortality that different places had seen before 1917, which helped to make sure that any

differences were down to responses to the 1918 pandemic specifically and not just different regions' exposure to imported infectious diseases generally.

More lockdowns, better growth

Cities that responded faster and more aggressively to the pandemic had better growth in employment and manufacturing output compared to cities with weaker responses. On average, cities that responded eight days earlier had four percent higher employment after the pandemic compared to cities that responded later. And cities that kept their measures in place for an extra six weeks or so had, on average, six percent higher employment afterward.

There are some important uncertainties in this analysis. For one thing, there was a huge range of outcomes in the cities that Correia and colleagues studied. The speed and aggression of each city's pandemic response can explain some of the difference in those outcomes, but there's a lot more to understand. Seattle, for instance, responded about as quickly as Cincinnati but had much better growth afterward. That doesn't change anything about the finding of the correlation, but it does mean that there's much more to the story to uncover in future research. It will be important to figure out what else played a role in economic resilience.

And, of course, the 1918 pandemic is not a perfect proxy for what's happening right now. It came at the end of a world war and killed huge numbers of working-age people. The different nature of the modern economy, with its communications technology, global supply chains, and dependence on services other than manufacturing, makes it difficult to understand how these responses will translate a century later.

But as with a lot of coronavirus research, uncertainty is unavoidable. The past can still be a useful guide, if not an exact template. And that past shows clearly that lockdowns

don’t inevitably lead to worse economic outcomes—and that there’s a strong chance they’re the best option for both lives and the economy.

https://arstechnica.com/?p=1667141

Company prioritizes $15k ventilators over cheaper model specified in contract



Enlarge / A mechanical ventilator developed in the University of Costa Rica (UCR) to be used for patients infected with CIVID-19, is tested in San Jose, on April 2, 2020. Universities and investigations centers in Costa Rica, Guatemala, Honduras and El Salvador have advanced on the

creation of prototypes of artificial ventilators, which if approved by sanitary authorities, could be manufactured by private companies for local hospitals in case of an explosion of the cases of the new coronavirus.
Ezequiel Becerra | Getty Images

reader comments

124 with 67 posters participating

Share this story

The Dutch company that received millions of taxpayer dollars to develop an affordable ventilator for pandemics but never delivered them has struck a much more lucrative deal with the federal government to make 43,000 ventilators at four times the price.

The US Department of Health and Human Services announced Wednesday that it plans to pay Royal Philips N.V. $646.7 million for the new ventilators—paying more than $15,000 each. The first 2,500 units are to arrive before the end of May, HHS said, and the rest by the end of December.

Philips refused to say which model of ventilator the government was buying. But in response to questions from ProPublica, HHS officials said the government is purchasing the Trilogy EV300, the more expensive version of the ventilator that was developed with federal funds.

The deal is a striking departure from the federal contract Philips' Respironics division signed in September to produce 10,000 ventilators for the Strategic National Stockpile at a cost of $3,280 each.

"This kind of profiteering—paying four times the negotiated price—is not only irresponsible to taxpayers but is particularly offensive when so many people are out of work," said Dr. Nicole Lurie, who served as the HHS assistant

secretary for preparedness and response during the Obama administration. “And besides, most of these ventilators will come too late to make a difference in this pandemic. We’ll then ’replenish’ the stockpile at a ridiculously high price.”

“What else,” she asked, “won’t we be able to buy as a result?”

In an article March 30, ProPublica detailed how the agency’s Biomedical Advanced Research and Development Authority, known as BARDA, had anticipated a decade ago that hospitals would run short of life-saving ventilators in the event of a pandemic. BARDA tried to find a company that could produce an inexpensive, durable ventilator that could be operated by people with minimal training during a crisis. After a deal with one company fell apart, HHS in 2014 agreed to pay Philips $13.8 million to design the stockpile ventilator with an option to purchase 10,000 for $3,280 each. The company won Food and Drug Administration clearance for its Trilogy Evo Universal ventilator in July, and in September HHS put in its order.

But Philips didn’t deliver any ventilators to the stockpile even as the coronavirus spread across the globe and hospitals scrambled for ventilators to keep their patients alive. Rather than making the government-funded design, Philips has been manufacturing more expensive commercial versions of the Trilogy Evo at its Pennsylvania plant and selling them overseas and in the United States.

Philips said it was within its rights to sell the commercial versions first because its contract with HHS gave the company until 2022 to produce the cheaper stockpile version. Philips had only made the stockpile version in small batches and didn’t want to ramp up production on a ventilator that it hadn’t mass produced, a slower process than increasing production of other models, company spokesman Steve Klink explained last month. He also said the government contract did not cover all of the costs for the ventilators’ development.

Now the company won’t have to try. The Philips contract announced Wednesday is for the commercial version, the Trilogy EV300, with the government paying $15,039 each.

The HHS statement said the agency purchased “what was immediately available” under “negotiated pricing” with Philips. President Donald Trump directed HHS Secretary Alex Azar to invoke the Defense Production Act in brokering the deal, the statement said.

The government still expects Philips to produce the 10,000 stockpile versions of the ventilator, but no completion date was given in the statement.

Lurie was in charge of the HHS office that struck the 2014 deal with Philips. During her time, congressional Republicans elected on a Tea Party wave forced cuts in federal spending that hampered efforts to bulk up the stockpile. The goal of the Philips deal, Lurie said, was to produce a low-cost, easy-to-use ventilator and use the stockpile’s budget responsibly. But it was also an effort to show the industry that low-cost ventilators were feasible.

“This was a strategy to reduce health care costs,” Lurie said. “This feels like a conspiracy to keep them high.”

In a news release touting the deal on Wednesday, Philips said that it has been ramping up production and this year has delivered several thousand ventilators to US hospitals—including one in hard-hit New York City. The company, which only makes ventilators in the US, said it wanted to continue selling ventilators to other countries in need. Klink declined to comment further.

John Hick, an emergency medicine specialist in Minneapolis who has advised HHS on pandemic response, said it would have been better to have a simpler and cheaper ventilator on hand.

“Don’t get me wrong, I am happy they are getting ventilators,”

he said. “If you could buy four times as many for the price, why wouldn’t you do that?”

Hick hopes that federal officials will learn a lesson from the Philips deal.

“We have lost a lot of time,” he said. “It’s kind of like telling someone we are going to hurricane-proof your house after the hurricane has hit.”

Update: The headline was changed after publication to provide more clarity on the contents fo the story.

https://arstechnica.com/?p=1667377

Citing BGP hijacks and hack attacks, feds want China Telecom out of the US



reader comments

71 with 40 posters participating, including story author

Share this story

Citing the misrouting of US Internet traffic, malicious hacking, and control by the Chinese government, a group of US executive agencies is recommending the FCC revoke the license authorizing China Telecom to provide international telecommunications services to and from the United States.

The recommendation comes amid an escalation in tensions between the US and China over a host of issues, including trade, disagreements about the handling of the novel coronavirus, and hacking. Thursday's move comes as part of a review the FCC disclosed last year, when the agency barred China Mobile Limited from the US market. The federal

government has also designated both Huawei and ZTE as national security threats.

“The security of our government and professional communications, as well as of our most private data, depends on our use of trusted partners from nations that share our values and our aspirations for humanity,” John C. Demers, assistant attorney general for national security, said in a release. “Today’s action is but our next step in ensuring the integrity of America’s telecommunications systems.”

The state-owned China Telecom says it’s the country’s second-biggest mobile operator with about 336 million subscribers, about 153 million wireline broadband subscribers, and about 111 million access lines. China Telecom Americas, the subsidiary that operates in the US, received authorization from the FCC in 2002, according to this timeline. China Telecom Americas has had a compounded and impressive annual revenue growth rate of 68 percent since 2005, the timeline added.

Hijacking huge swaths of the Internet

Over the past decade, the Chinese telecom has been at the center of several major security events, most visibly those involving the misrouting of huge chunks of Internet traffic sent to and from the US and other countries.

One of the more concerning events came to light in 2018 when a researcher revealed that China Telecom had diverted US domestic Internet communications to mainland China before sending them on to their intended destinations. The improper paths—which were the result of manipulations to border gateway protocol tables that route traffic from one backbone provider to another—occurred over a two-and-a-half-year span, from 2015 to 2017.

Another BGP mishap occurred in 2019 when China Telecom diverted traffic destined for some of Europe's biggest mobile providers for two hours. A third event in 2014 repeatedly sent traffic traveling inside the borders of Russia through China Telecom servers. There's conflicting evidence about whether the latter two incidents were malicious hijackings or accidental routing leaks.

BGP is largely based on implicit trust one provider—which in Internet parlance is known as an AS or autonomous system—places in another. These ASes "announce routes" that other ASes should use to reach networks in particular geographic regions. While BGP favors the shortest, most direct paths, erroneous or malicious announcements can cause traffic to follow roundabout paths that can cause major outages or worse. BGP hijackings are especially concerning because they allow spies from China, Russia, or elsewhere to monitor or tamper with any unencrypted data that improperly passes through their networks before being sent on to the intended destination.

A decade of high-profile hacks

US government officials have other concerns. Hacking groups widely believed to work on behalf of the Chinese government have been active in attacks against the US and its allies. One group that's known under a variety of names, including LEAD, BARIUM, Wicked Panda, GREF, PassCV, Axiom, and Winnti, is behind a decade of malicious hacks, according to a report released in 2018. The Chinese government has also been tied to attacks on satellite, defense, and telecom firms, the Federal Deposit Insurance Corporation, and Google, to name only a few.

Thursday's recommendation was jointly issued by the Departments of Justice, Homeland Security, Defense, State, Commerce, and the United States Trade Representative. The release cited the following basis for the recommendation:

- the evolving national security environment since 2007 and increased knowledge of the PRC's role in malicious cyber activity targeting the United States;
- concerns that China Telecom is vulnerable to exploitation, influence, and control by the PRC government;
- inaccurate statements by China Telecom to US government authorities about where China Telecom stored its US records, raising questions about who has access to those records;
- inaccurate public representations by China Telecom concerning its cybersecurity practices, which raise questions about China Telecom's compliance with federal and state cybersecurity and privacy laws; and
- the nature of China Telecom's US operations, which provide opportunities for PRC state-actors to engage in malicious cyber activity enabling economic espionage and disruption and misrouting of US communications.

In a statement, officials with China Telecom Americas wrote:

> *Today, several government agencies took the procedurally unprecedented step of making allegations related to China Telecom Americas' FCC licensing. We unequivocally deny the allegations. The company has always been extremely cooperative and transparent with regulators. In many instances, we have gone beyond what has been requested to demonstrate how our business operates and serves our customers following the highest international standards. We look forward to sharing additional details to support our position and addressing any concerns.*

US governmental officials and some researchers disagree and say that China's offensive hacking is extensive.

Complicating matters, attributing hacks to specific groups or countries is notoriously difficult, since attackers frequently

plant false flags that wrongly implicate rivals. What's more, BGP routing mishaps happen repeatedly and frequently as a result of error and not malice. Earlier this week, for instance, an exchange of routing information between Russian providers Rascom (AS 20764) and Rostelecom (AS 12389) caused traffic to be improperly routed through Russia. The event lasted for about seven minutes and affected some of the biggest names on the Internet including Cloudflare, Amazon, Akamai, Digital Ocean, Linode, Hetzner, OVH, Leaseweb, Softlayer, Portlane, Fastly, and Ali Baba. Two BGP experts, who asked not to be named because their employers didn't authorize them to speak on the record, said all evidence points to the misrouting being the result of a configuration error.

And in cases when BGP events are the work of China or other countries, kicking their telecoms out of the US does little to stop hijackings.

"BGP hijacks can be conducted from anywhere and don't require [physical presence] in the US," one of the experts said. "Which makes this move seem more like punishment or retribution than a move that would actually stop hijacks."

https://arstechnica.com/?p=1667334

Some shirts hide you from cameras—but will anyone wear them?



Aurich Lawson / Getty

reader comments

119 with 83 posters participating, including story author

Share this story

Right now, you're more than likely spending the vast majority of your time at home. Someday, however, we will all be able to leave the house once again and emerge, blinking, into society to work, travel, eat, play, and congregate in all of humanity's many bustling crowds.

The world, when we eventually enter it again, is waiting for us with millions of digital eyes—cameras, everywhere, owned by governments and private entities alike. Pretty much every state out there has some entity collecting license plate data from millions of cars—parked or on the road—every day. Meanwhile all kinds of cameras—from police to airlines, retailers, and your neighbors' doorbells—are watching you every time you step outside, and unscrupulous parties are offering facial recognition services with any footage they get their hands on.

In short, it’s not great out there if you’re a person who cares about privacy, and it’s likely to keep getting worse. In the long run, pressure on state and federal regulators to enact and enforce laws that can limit the collection and use of such data is likely to be the most efficient way to effect change. But in the shorter term, individuals have a conundrum before them: can you go out and exist in the world without being seen?

Systems are dumber than people

You, a person, have one of the best pattern-recognition systems in the entire world lodged firmly inside your head: the human brain.

People are certainly easy to fool in many ways—no argument there. But when it comes to recognizing something as basic as a car, stop sign, or fellow human being—literally the kinds of items that babies and toddlers learn to identify before they can say the words—fooling cameras is in many ways easier than fooling people. We’re simply trained by broad experience to look at things differently than software is.

For example, if you’re driving down the road and see a stop sign at night, you still know it’s supposed to be “red.” And if it has some weird stickers on it, to you it is still fundamentally a stop sign. It’s just one that someone, for some reason, has defaced. A car, however, may instead “read” that sign as a speed limit sign, indicating it should go up to 45 miles per hour, with potentially disastrous results.

Similarly, a person looking at another person with a weird hairstyle and splotches of makeup on their face will see a human, sporting a weird hairstyle and with makeup on their face. But projects such as CV Dazzle have shown that, when applied in a certain way, makeup and hair styling can be used to make a person effectively invisible to facial recognition systems.

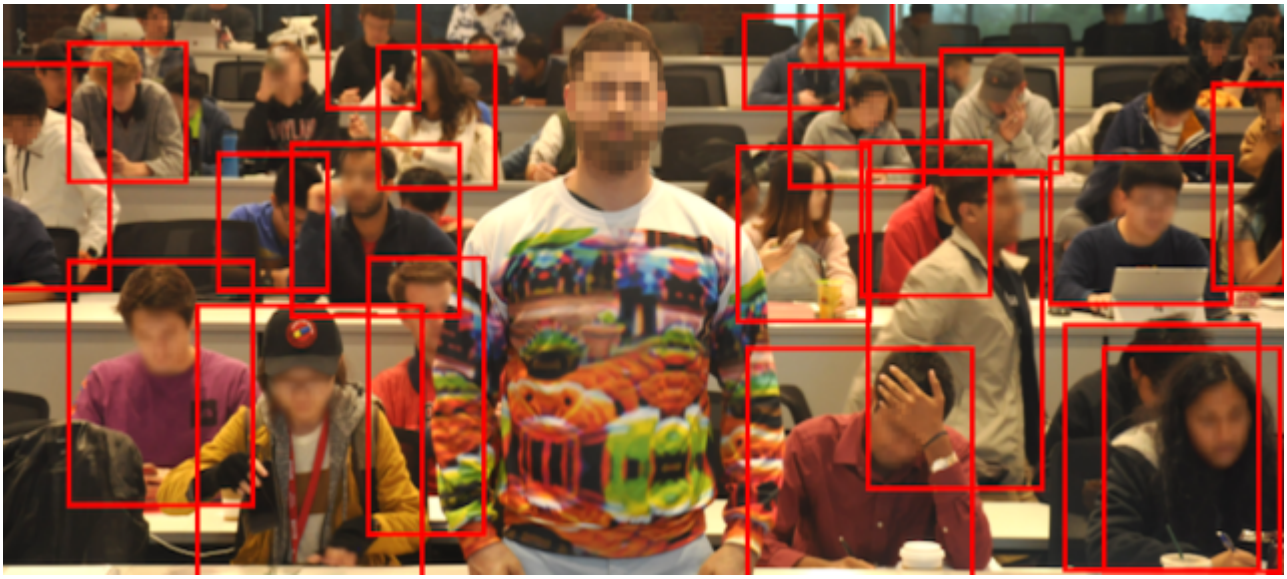
Heavy, patterned makeup and hair straight out of a JRPG are impractical for daily life, but all of us put on some kind of clothing to leave the house. As Ars' own Jonathan Gitlin has described, the idea of using the "ugly shirt" to render oneself invisible to cameras has been a part of science fiction for a decade or more. But today, there are indeed computer scientists and artists working to make invisibility as simple as a shirt or a scarf… in theory, at least.

Digital and physical invisibility

Two decades of *Harry Potter* in the public imagination have cemented for millions the idea that a cloak of invisibility itself should be lightweight and hard to perceive. The reality, on the other hand, is not exactly subtle—and still very much a work in progress.

"If you wanted to do like a *Mission Impossible*-style heist of the Smithsonian, I don't think you'd want to rely on this cloak to not be detected by a security system," computer science professor Tom Goldstein, of the University of Maryland, told Ars in an interview.

Goldstein and a team of students late last year published a paper studying "adversarial attacks on state-of-the-art object detection frameworks." In short, they looked at how some of the algorithms that allow for the detection of people in images work, then subverted them basically by tricking the code into thinking it was looking at something else.



Enlarge / The bright adversarial pattern, which a human viewer can darn-near see from space, renders the wearer invisible to the software looking at him.

It turns out, confounding software into not realizing what it's looking at is a matter of fooling several different smaller systems at once.

Think about a person, for example. Now think of a person who looks nothing like that. And now do it again. Humanity, after all, contains multitudes, and a person can have many different appearances. A machine learning system needs to understand the diverse array of different inputs that, put together, mean "person." A nose by itself won't do it; an eye alone will not suffice; anything could have a mouth. But put dozens or hundreds of those priors together, and you've got enough for an object detector.

Code does not "think" in terms of facial features, the way a human does, but it does look for and classify features in its own way. To foil it, the "cloaks" need to interfere with most or all of those priors. Simply obscuring some of them is not enough. Facial recognition systems used in China, for example, have been trained to identify people who are wearing medical masks while trying to prevent the spread of COVID-19 or other illnesses.

And of course, to make the task even more challenging,

different object detection frameworks all use different mechanisms to detect people, Goldstein explained. “We have different cloaks that are designed for different kinds of detectors, and they transfer across detectors, and so a cloak designed for one detector might also work on another detector,” he said.

But even when you get it to work across a number of different systems, making it work *consistently* is another layer.

“One of the things we did in our research was to quantify how often these things work and the variability of the scenarios in which they work,” he said. “Before, they got it to work once, and if the lighting conditions were different, for example, maybe it doesn’t work anymore, right?”

People move. We breathe, we turn around, we pass through light and shadow with different backgrounds, patterns, and colors around us. Making something that works when you’re standing in a plain white room, lit for a photo session, is different from making something that works when you’re shopping in a big-box store or walking down the street. Goldstein explained:

> *Modifying an image is different than modifying a thing, right? If you give me an image, I can say: we’ll make this pixel intensity over here different, make that pixel intensity over there a little more red, right? Because I have access to the pixels, I can change the individual bits that encode that image file.*
>
> *But when I make a cloak, I don’t have that ability. I’m going to make a physical object and then a detector is going to input the image of me and pass the result to a computer. So when you have to make an adversarial attack in the physical world, it has to survive the detection process. And that makes it much more difficult to craft reliable attacks.*

All of the digital simulations run on the cloak worked with

100-percent effectiveness, he added. But in the real world, “the reliability degrades.” The tech has room for improvement.

“How good can they get? Right now I think we’re still at the prototype stage,” he told Ars. “You can produce these things that, when you wear them in some situations, they work. It’s just not reliable enough that I would tell people, you know, you can put this on and reliably evade surveillance.”

https://arstechnica.com/?p=1662453