# 50 states and territories launch massive joint probe into Google

Enlarge / District of Columbia Attorney General Karl Racine (L) and Texas Attorney General Ken Paxton speak during the launch of an antitrust investigation into large tech companies, outside of the US Supreme Court in Washington, DC, on September 9, 2019.

## reader comments

156 with 82 posters participating

## Share this story

A coalition of attorneys general representing 50 US states and territories today announced a long-awaited joint probe into antitrust complaints against one of the biggest tech companies in the world, Google.

The office of Texas Attorney General Ken Paxton is spearheading the bipartisan investigation, which is beginning with the search and digital advertising markets. Google "dominates all aspects of advertising on the Internet and searching on the Internet," Paxton told reporters during a press conference.

The group includes attorneys general from 48 states, Puerto Rico, and the District of Columbia. (Alabama and California are the two states not participating.) The states' action is independent of several different federal actions, participating attorneys general stressed.

“I’m very confident that this bipartisan group is going to be led by the facts and not be swayed by any conclusion that may fall short, if you will, if it’s inconsistent with our facts, on the federal side,” DC Attorney General Karl Racine said. “So we’re going to do what we think is right based on our investigation.”

Utah Attorney General Sean Reyes added, “there’s nothing wrong with being a dominant player when it’s done fairly,” but the “pervasiveness” of complaints about Google indicates the company may not be behaving fairly.

Florida Attorney General Ashley Moody echoed the sentiment. “When there is no longer a free market or competition, this increases prices, even when something is marketed as free, and harms consumers,” Moody said. “Is something really free if we are increasingly giving over our privacy information?”

## Here we go again

Google’s attorneys are extremely familiar with handling antitrust probes by now.

The Justice Department publicly confirmed in July its antitrust division was digging into widespread “concerns that consumers, businesses, and entrepreneurs have expressed” about “market-leading online platforms.” The agency, which rarely comments publicly on pending probes, didn’t name names, but several media reports have suggested that the DOJ and Federal Trade Commission agreed to split the big antitrust work this year, with the DOJ taking on Apple and Google while the FTC looks at Amazon and Facebook.

“We have answered many questions on these issues over many years, in the United States as well as overseas, across many aspects of our business, so this is not new for us,” Google exec Kent Walker wrote last week in a blog post confirming that the company is the target of a DOJ probe.

The FTC has been contemplating antitrust action against Google for the better part of a decade. In 2012, a memo circulated to all five commissioners strongly recommended launching an antitrust suit against Google for abusing its dominance. In 2013, the commission voted against bringing charges, leading to several years of criticism.

The European Commission's competition bureau, which handles antitrust matters for the European Union, has fined Google billions of dollars across three years for antitrust violations. First came a then-record-breaking €2.42 billion fine in 2017 for steering shoppers toward Google's platform in search results. That record was then broken in 2018 with a €4.34 billion fine for unfairly pushing its own apps ahead of competitors', and those two fines were joined by another €1.5 billion this year for abusing its dominant position in the ad sales market.

## Misery loves company?

Google is accustomed to antitrust probes, after the several past and present investigations and actions against it. But the Internet giant is far from the only major business facing serious complaints this year.

Facebook also confirmed in July that it is under antitrust investigation by the FTC, and last week a coalition of attorneys general representing eight states and the District of Columbia also launched a probe, led by Attorney General Letitia James of New York.

Amazon, too, is at the heart of a boatload of investigations. Retailers have all but begged for US regulators to take strong action, joining Germany, Austria, Italy, and the European Union, which all have their own antitrust probes going on right now.

Congress in June launched a bipartisan investigation looking

at “competition in digital markets.” The investigation—which has probed Facebook, Google, and Amazon so far—went quiet during the traditional August recess, but several hearings on the topic are slated for later this month.

Apple is also reportedly the target of investigations. Music-streaming service Spotify lodged a complaint with the EU about Apple’s app-store behavior. The Congressional probe also started asking about Apple’s position on consumers’ right to repair their own devices as part of its work.

https://arstechnica.com/?p=1564297

---

# Chinese professor stole hard drive secrets for Huawei, US government charges

Enlarge / Visitors check out new Huawei smartphones at the 2019 IFA home electronics and appliances trade fair Berlin.
Sean Gallup/Getty Images

## reader comments

96 with 58 posters participating, including story author

## Share this story

A Chinese computer science professor named Bo Mao is facing wire fraud charges after he was arrested last month by US authorities.

The document formally charging Mao in Brooklyn federal court charges that he conspired to "defraud a company headquartered in the Northern District of California." Other court filings, including a criminal complaint filed in a Texas federal court last month, help fill in the details. As Reuters first reported, Mao is accused of stealing trade secrets from a startup called CNEX Labs on behalf of Chinese telecommunications giant Huawei.

The prosecution is the latest effort by the Trump administration to punish Huawei for alleged industrial espionage. In January, the US government indicted Huawei after employees attempted to steal proprietary information about a T-Mobile robot used to test mobile phones.

Huawei blasted the US government for what it viewed as a biased pattern of prosecutions. "US federal prosecutors are charging forward with CNEX's allegations" even though a civil trial resulted in no damages against Huawei, the company noted in a statement to Reuters.

## Feds say Mao stole secrets for Huawei

Huawei and CNEX have been fighting in court for years. One of the startup's co-founders, Yiren Huang, started CNEX just days after quitting his job at Huawei. Huawei sued Huang in 2017 over alleged trade secret theft. CNEX countered with accusations of its own. The legal battle between the two firms ended in a draw this summer, with a jury finding that neither side owed damages.

But Mao now faces criminal prosecution for allegedly helping Huawei steal trade secrets. Mao allegedly convinced CNEX to ship him a prototype of one of its products, a controller board for solid-state drives. Mao promised not to reverse-engineer the board or provide details about it to third

parties. But the government charges that Mao did exactly that.

Mao is a professor at Xiamen University in China, but he is also listed as a research associate or postdoc on the website of Hong Jiang, a professor at the University of Texas – Arlington.

In an August complaint filed in a Texas federal court, an FBI agent charges that Mao worked with “Professor 1” at a “Texas University” to obtain device samples from a “victim company.” The complaint notes that “Company 1” made a $100,000 gift to “the Texas University” to allow “Professor 1” to study “Enforcing Xth Percentile Latency and Throughput SLOs under Consolidated Datacenter Resources.”

Hong Jiang lists a research project with that exact title on his university home page, with Futurewei—a subsidiary of Huawei—listed as the sponsor.

The FBI says that it obtained email records showing that Mao and Huawei conferred regularly as Mao attempted to reverse engineer the CNEX device.

https://arstechnica.com/?p=1564163

---

# Algorithms should have made courts more fair. What went wrong?

Enlarge / The courts have become another frontline in the

battle against climate change.

## reader comments

122 with 82 posters participating

## Share this story

Kentucky lawmakers thought requiring that judges consult an algorithm when deciding whether to hold a defendant in jail before trial would make the state’s justice system cheaper and fairer by setting more people free. That’s not how it turned out.

Before the 2011 law took effect, there was little difference between the proportion of black and white defendants granted release to await trial at home without cash bail. After being mandated to consider a score predicting the risk a person would reoffend or skip court, the state’s judges began offering no-bail release to white defendants much more often than to blacks. The proportion of black defendants granted release without bail increased only slightly, to a little over 25 percent. The rate for whites jumped to more than 35 percent. Kentucky has changed its algorithm twice since 2011, but available data shows the gap remained roughly constant through early 2016.

The Kentucky experience, detailed in a study published earlier this year, is timely. Many states and counties now calculate “risk scores” for criminal defendants that estimate the chance a person will reoffend before trial or skip court; some use similar tools in sentencing. They are supposed to help judges make fairer decisions and cut the number of people in jail or prison, sometimes as part of eliminating cash bail. Since 2017, Kentucky has released some defendants scored as low-risk based purely on an algorithm’s say-so, without a judge being involved.

How these algorithms change the way justice is administered is largely unknown. Journalists and academics have shown that risk-scoring algorithms can be unfair or racially biased. The more crucial question of whether they help judges make better decisions and achieve the tools' stated goals is largely unanswered.

The Kentucky study is one of the first in-depth, independent assessments of what happens when algorithms are injected into a justice system. It found that the project missed its goals and even created new inequities. "The impacts are different than what policymakers may have hoped for," says Megan Stevenson, a law professor at George Mason University who authored that study.

Stevenson looked at Kentucky in part because it was a pioneer of bail reform and algorithm-assisted justice. The state began using pretrial risk scores in 1976, a simple system that assigned defendants points based on questions about their employment status, education, and criminal record. The system was refined over time, but the scores were used inconsistently. In 2011, a law called HB 463 mandated their use for judges' pretrial decisions, creating a natural experiment.

Kentucky's lawmakers intended HB 463 to reduce incarceration rates, a common motivation for using risk scores. They are supposed to make judges better at assessing who is safe to release. Sending a person home makes it easier for them to continue their work and family life and saves the government money. More than 60 percent of the 730,000 people held in local jails in the US have not been convicted, according to the nonprofit Prison Policy Initiative.

The system used in Kentucky in 2011 employed a point system to

produce a score estimating the risk that a defendant will skip their court date or reoffend before trial. A simple framework translated the score into a rating of low-, moderate-, or high-risk. People tagged as low- or moderate-risk generally should be released without cash bail, the law says.

But judges appear not to have trusted that system. After the law took effect, they overruled the system's recommendation more than two-thirds of the time. More people got sent home, but the increase was small; around the same time, authorities reported more alleged crimes by people on release pending trial. Over time, judges reverted to their prior ways. Within a couple of years, a smaller proportion of defendants was being released than before the bill came into force.

Although more defendants were granted release without bail, the change mostly helped white people. "On average white defendants benefited more than black defendants," Stevenson says. The pattern held after Kentucky adopted a more complex risk-scoring algorithm in 2013.

One explanation supported by Kentucky data, she says, is that judges responded to risk scores differently in different parts of the state. In rural counties, where most defendants were white, judges granted release without bond to significantly more people. Judges in urban counties, where the defendant pool was more mixed, changed their habits less.

A separate study using Kentucky data, presented at a conference this summer, suggests a more troubling effect was also at work. It found that judges were more likely to overrule the default recommendation to waive a financial bond for moderate-risk defendants if the defendants were black.

Harvard researcher Alex Albright, who authored that study, says it shows more attention is needed to how humans interpret algorithms' predictions. "We should put as much effort into how we train people to use predictions as we do into the

predictions," she says.

Michael Thacker, risk-assessment coordinator with Kentucky pretrial services, said his agency tries to mitigate potential bias in risk-assessment tools and talks with judges about the potential for "implicit bias" in how they interpret the risk scores.

An experiment that tested how judges react to hypothetical risk scores for determining sentences also found evidence that algorithmic advice can cause unexpected problems. The study, which is pending publication, asked 340 judges to decide sentences for made-up drug cases. Half of the judges saw "cases" with risk scores estimating the defendant had a medium to high risk of rearrest and half did not.

When they weren't given a risk score, judges were tougher on more-affluent defendants than poor ones. Adding the algorithm reversed the trend: Richer defendants had a 44 percent chance of doing time but poorer ones a 61 percent chance. The pattern held after controlling for the sex, race, political orientation, and jurisdiction of the judge.

"I thought that risk assessment probably wouldn't have much effect on sentencing," says Jennifer Skeem, a UC Berkeley professor who worked on the study with colleagues from UC Irvine and the University of Virginia. "Now we understand that risk assessment can interact with judges to make disparities worse."

There is reason to think that if risk scores were implemented carefully, they could help make the criminal justice system fairer. The common practice of requiring cash bail is widely acknowledged to exacerbate inequality by penalizing people of limited means. A National Bureau of Economic Research study from 2017 used past New York City records to project that an algorithm predicting whether someone will skip a court date could cut the jail population by 42 percent and shrink the

proportion of black and Hispanic inmates, without increasing crime.

Unfortunately, the way risk-scoring algorithms have been rolled out across the US is much messier than in the hypothetical world of such studies.

Criminal justice algorithms are generally relatively simple and produce scores from a small number of inputs such as age, offense, and prior convictions. But their developers have sometimes restricted government agencies using their tools from releasing information about their design and performance. Jurisdictions haven't allowed outsiders access to the data needed to check their performance.

"These tools were deployed out of reasonable desire for evidence-based decision making, but it was not done with sufficient caution," says Peter Eckersley, director of research at Partnership on AI, a nonprofit founded by major tech companies to examine how the technology affects society. PAI released a report in April that detailed problems with risk assessment algorithms and recommended agencies appoint outside bodies to audit their systems and their effects.

Stevenson agrees that greater transparency is needed—but also admits to feeling it may be too late to turn risk-scoring algorithms into a success, given their poor reputation and the slim gains they seem to offer. "The criminal justice system has such little good will already that I don't want people to lose any more hope or faith at this point," she says.

*This story originally appeared on wired.com.*

https://arstechnica.com/?p=1564003

# Trump admin threatens California, automakers over emissions deal

Enlarge / Traffic moves through an interchange along Interstate 580 on July 25, 2019 in Oakland, California.

## reader comments

161 with 97 posters participating

## Share this story

Four major automakers that recently reached an agreement with the state of California to hold to certain emissions standards over the next decade are now the target of a federal antitrust investigation.

Ford, Honda, BMW, and Volkswagen confirmed to media they have been contacted about the probe, which was first reported by The Wall Street Journal.

“Honda will work cooperatively with the Department of Justice with regard to the recent emissions agreement reached between the State of California and various automotive manufacturers, including Honda,” the company said. BMW and Ford also confirmed receiving a letter from the DOJ, and Volkswagen said it is in “regular contact” with US authorities.

The companies reached an agreement with the California Air Resource Board (CARB) in July to produce cars for the US market that exceed national level-fuel efficiency standards. Under the terms of the deal, the automakers will improve their overall fleets’ average fuel efficiency by 3.7% per year,

starting with the 2022 model year. The plan also includes certain incentives to promote a transition to widespread manufacture and adoption of electric vehicles.

In a separate action from the DOJ probe, the Environmental Protection Agency and Department of Transportation also sent a letter (PDF) to "put California on notice."

"This framework agreement appears to be inconsistent with Federal law," the agencies said. "We urge you to act immediately to disassociate CARB from the commitments made by the four automakers. Those commitments may result in legal consequences given the limits placed in Federal law on California's authority."

State leadership, however, does not appear likely to give way in response to the threat. "The Trump Administration has been attempting and failing to bully car companies for months now," California Governor Gavin Newsom said in an emailed statement. "We remain undeterred. California stands up to bullies and will keep fighting for stronger clean car protections that protect the health and safety of our children and families."

CARB chairwoman Mary D. Nichols in an emailed statement said the DOJ "brings its weight to bear against auto companies in an attempt to frighten them out of voluntarily making cleaner, more efficient cars and trucks than EPA wants. Consumers might ask, who is [EPA Administrator] Andy Wheeler protecting?"

# Trump vs efficiency

The deal the automakers agreed to with CARB echo a standard set by the Environmental Protection Agency in 2012, which called for gradually increasing the average miles-per-gallon rating for most cars to 54.5mpg by 2025 (about 40mpg under real-world conditions). Like many other Obama-era standards, however, such as methane emissions limits or lightbulb standards, the EPA's fuel efficiency rule became an early

target of the Trump administration.

Federal regulators do indeed have the statutory right to set national fuel-efficiency guidelines, as the EPA and DOT wrote. California, however, is historically something of a special case. The state, which used to suffer from an extreme smog problem, has for several decades had a waiver allowing it to set more stringent fuel-efficiency guidelines than federal law calls for. When the EPA rolled back the 2012 standard, California fought back.

For a brief time, the Trump administration was theoretically negotiating with CARB to search for a compromise position, but those talks never amounted to much, and they completely collapsed in February.

California law is critical to carmakers because emissions regulations in California spread far beyond the Golden State's borders. Most states can't set their own fuel-efficiency guidelines; California is a special case. While the other 49 states in the union are not allowed to set their own fuel efficiency standards, they *can* choose to adopt California's stricter limits instead of the federal guideline. At least 16 said earlier in the year they would choose California's rather than support the federal rollback.

Ford, Honda, BMW, and Volkswagen are all among the 17 automakers that asked the Trump administration in June to negotiate with California to find a single, unified national standard.

Although the four companies agreed to stricter, voluntary terms with California, "a 50-state solution has always been our preferred path forward," they said in a joint statement. "These terms will provide our companies much-needed regulatory certainty by allowing us to meet both federal and state requirements with a single national fleet, avoiding a patchwork of regulations while continuing to ensure meaningful

greenhouse gas emissions reductions."

https://arstechnica.com/?p=1563675

---

# Facebook on the hook as states launch competition, privacy probe

NurPhoto | Getty Images

## reader comments

23 with 18 posters participating, including story author

## Share this story

A coalition of states attorneys general is joining together to launch yet another antitrust probe of Facebook, joining several investigations already in progress.

"I'm launching an investigation into Facebook to determine whether their actions endangered consumer data, reduced the quality of consumers' choices, or increased the price of advertising," New York attorney general Letitia James said this morning. "The largest social media platform in the world must follow the law."

The bipartisan group will determine whether Facebook used its market dominance to unfairly stifle competition. It will also examine if Facebook took anticompetitive actions that harm

consumer data and privacy, “the quality of consumers’ choices,” and pricing in the digital advertising market. Attorneys general for Colorado, Florida, Iowa, Nebraska, North Carolina, Ohio, Tennessee, and the District of Columbia are also participating, James’s office said in a press release.

## A crowded field

Facebook cofounder Chris Hughes has been making the rounds in Washington explaining why he thinks the company should break up, and he seems at least to have an interested audience. The states are just the latest set of regulators to use the lens of antitrust law to take a deep look at Facebook’s behavior and market dominance.

The Department of Justice publicly confirmed in July that the antitrust division had begun probing the widespread “concerns that consumers, businesses, and entrepreneurs have expressed” about “market-leading online platforms.” The agency didn’t name names but the shortlist of “market-leading” platforms that qualify is generally considered to comprise Amazon, Apple, Facebook, and Google.

Facebook told investors in July that it was the target of an open antitrust investigation by the Federal Trade Commission. Congress also launched its own series of antitrust hearings in June looking at “competition in digital markets.” The investigation, which has bipartisan backing, went quiet during the August Congressional recess, but the House and Senate between them have several antitrust hearings scheduled for later this month.

Facebook’s global reach—the behemoth now boasts 2.4 billion monthly active users, or just a little under a third of the Earth’s population—also makes it susceptible to global investigation. The European Commission’s competition bureau is also actively probing Facebook for antitrust reasons, according to media reports, while member states such as

Germany are also taking action. Australian regulators also think they should maybe have a closer look.

The coming years could also get more challenging for the company depending how the political winds blow. Sen. Elizabeth Warren (D-Mass.) made a pledge to break up big tech platforms, including Facebook, one of her major policy proposals earlier this year as she seeks to be the Democratic nominee for the 2020 presidential race.

https://arstechnica.com/?p=1563449

---

# China is close to releasing a Libra-like digital currency

Enlarge / An employee counts 100-yuan notes at a bank in Nantong in China’s eastern Jiangsu province on July 23, 2018. -/AFP/Getty Images

## reader comments

79 with 53 posters participating

## Share this story

China’s central bank is working on a cryptocurrency that will be similar to Facebook’s Libra, a government official said this week, according to Reuters.

China’s central bank has had a group studying digital currencies since at least 2014, but their efforts seem to have

come into focus in recent months. Last month, Mu Changchun, deputy director of the People's Bank of China's payments department, announced that an official Chinese digital currency was "almost ready."

Details about the technology remain scarce, but it seems that the new currency will—like Libra—be pegged to a conventional currency to maintain its value. While Libra will be linked to a basket of conventional currencies including the dollar and the euro, China's digital currency will be pegged to the yuan.

Mu said that the cryptocurrency was designed to "protect our monetary sovereignty and legal currency status." Government officials in the United States and overseas have raised concerns that if Libra gets traction, it could threaten the dominance of conventional currencies backed by governments.

Mu said that the currency would be usable on major Chinese messaging platforms like WeChat and AliPay. Libra, of course, is designed to be used on Facebook's own messaging products.

The currency could be issued by both China's central bank and financial institutions.

"Mu said China's digital currency would strike a balance between allowing anonymous payments and preventing money-laundering," Reuters reports.

https://arstechnica.com/?p=1563455

---

# T-Mobile Metro stores sell

# used phones as new, charge “fake taxes,” NYC says

Enlarge / The logo of Deutsche Telekom, owner of T-Mobile, seen at Mobile World Congress in February 2019 in Barcelona, Spain.

## reader comments

39 with 34 posters participating

## Share this story

The New York City government sued T-Mobile yesterday, alleging that its Metro stores routinely use “abusive sales tactics” such as selling used phones as if they are new and charging customers for services they didn’t order.

“Abusive sales tactics are rampant at Metro stores,” the complaint says. “At least several dozen have sold used phones to consumers as though they were new, charged consumers for fake taxes and unwanted services, or enrolled consumers in expensive financing plans without their consent.”

T-Mobile’s Metro division offers prepaid service over the T-Mobile wireless network and is branded as “Metro by T-Mobile.” It was known as MetroPCS until a 2018 rebranding. T-Mobile has stressed that Metro and itself are one and the same, announcing that “Metro by T-Mobile *is* T-Mobile,” the lawsuit noted.

The Metro by T-Mobile abuses “do not end at the store,” the NYC lawsuit says:

> *The Metro website, which is owned by T-Mobile and emblazoned*

> *with the "Metro by T-Mobile" logo, deceives consumers about its stingy return policy: it advertises a "30-day guarantee" on all Metro cell phone purchases, but the fine print reveals that returns or exchanges are only available for a small sub-category of transactions, and only within seven days of purchase.*
>
> *This illegal activity is pervasive, spanning 56 locations across all five boroughs of New York City, and includes both "authorized dealers" and stores directly operated by T-Mobile's subsidiary, MetroPCS NY. The deception costs consumers considerably. For example, of the 21 phones that DCA [New York City Department of Consumer Affairs] identified as used, most were iPhones that cost several hundred dollars each.*

The lawsuit was filed in the state Supreme Court for New York County. The NY Supreme Court is a trial-level court; New York's highest state court is the Court of Appeals.

## Thousands of violations

Defendants include T-Mobile, T-Mobile's MetroPCS New York division, and various owners of Metro stores. T-Mobile owns some Metro stores directly, while others are owned by dealers that "contract with MetroPCS NY for permission to operate under the Metro brand," the lawsuit said. The defendants "violated the City's Consumer Protection Law thousands of times," the city said in a press release today.

Metro stores charged "illegal taxes, mystery fees, and fees for unwanted services," the city said.

"Some Metro stores sell phones at a discount, but then add taxes on the much higher, pre-discount figure, which is illegal under state law," the city said. "Metro also charged several customers undisclosed and illegal activation fees, and

for unwanted products and services like GPS navigation, extra lines, and hotspot capability."

The city's lawsuit seeks forfeiture of revenue in order to create "a restitution fund to compensate New Yorkers scammed at Metro stores." The city said it is also seeking to have T-Mobile "notify all major credit bureaus that the financing contracts were fraudulent so that related information can be removed from the consumers' credit reports, and to pay civil penalties."

"Companies that blatantly scam New Yorkers must be held accountable," Mayor Bill de Blasio said in the city's press release. "We are doing everything in our power to make sure that T-Mobile ends these deceptive practices and that customers who were taken advantage of get the restitution they are owed."

When contacted by Ars, T-Mobile said it "take[s] these allegations very seriously" and is "continuing to investigate so we can respond to the City."

"Though we can't comment on the specific claims at this early stage, what we are seeing alleged here is completely at odds with the integrity of our team and the commitment they have to taking care of our customers every day," T-Mobile said.

## Used phones sold as new

Metro by T-Mobile stores "do not advertise that they sell used phones," but "dozens of NYC consumers in the last three years have complained that the phones they bought from NYC Metro Stores were used," the lawsuit says.

Some customers verified through Apple that their "new" phones purchased from Metro by T-Mobile had been previously activated, the lawsuit said. Others discovered that the phones were used because they were "covered in scratches" or could

not be charged, the lawsuit said.

When it came to financing agreements, Metro stores "deceived NYC consumers about things as basic as the actual price of the phone to things as complicated as the terms of financing," the lawsuit said. In one instance in January 2019, a consumer named Vashti Anais Wagner tried to buy a phone that was advertised for $599, but the Metro store allegedly enrolled her in a lease agreement in which she'd have to pay $2,191.30 in monthly installments of $199.21.

"The employee did not show Ms. Wagner the contract, appears to have e-signed it in her name, and did not tell her that she would be leasing the phone rather than buying it outright," the lawsuit said.

New York City said it found eight other instances in which Metro stores "simply lied to consumers about down payments or required monthly payments."

## 30-day guarantee "wholly illusory"

While Metro's website advertises a 30-day guarantee on phone purchases, Metro's actual return policy "only allows returns within *seven* days from in-store purchases—and *all purchases are in-store*, because it is impossible to buy a phone from the Metro Website," the lawsuit said. "The touted '30-day guarantee' is wholly illusory, and completely deceptive."

The return policy is also so restrictive that it "bars returns from consumers who bought the phone for an existing line of service or who have 'warranty issues,' which are not defined," the lawsuit said.

New York's lawsuit also said that Metro stores "overcharged consumers through deceptive representations about taxes and other fees, and by surreptitiously adding unwanted services to wireless plans and unexplained fees on consumer receipts."

A Metro store charged one customer what it called “sales taxes,” but the taxes went far beyond New York’s sales tax rate, “and it is unclear how they were calculated,” the lawsuit said.

Additionally, “Metro charged at least two other consumers undisclosed, illegal ‘activation payments’ of over $70 each, has overcharged at least one other consumer for SIM cards, and has overcharged at least four consumers by including unwanted services like GPS navigation, extra lines, or hotspot capability, in monthly wireless plans,” the lawsuit said.

Defendants were also accused of “fail[ing] to provide legal sales receipts.”

https://arstechnica.com/?p=1563047

---

# Senator pushes Amazon for details about Ring “partnerships” with police

Enlarge / A Ring video doorbell mounted on a home.

## reader comments

30 with 21 posters participating

## Share this story

Amazon’s Ring line of video doorbells and home surveillance

equipment is particularly popular with one key group: police. More than 400 law enforcement agencies around the country have partnered with Ring to use its apps and help market its security cameras to residents in the name of safer neighborhoods. As a dozen recent media reports have shown, however, the details about these partnerships and the privacy concerns they raise tend to be shrouded in secrecy and hard to learn.

Sen. Ed Markey (D-Mass.) is now among those who would like Amazon to explain what, exactly, Ring is up to. “The nature of Ring’s products and its partnerships with police departments raise serious privacy and civil liberties concerns,” Markey said in a letter (PDF) addressed to Amazon CEO Jeff Bezos.

“Although Amazon markets Ring as America’s ‘new neighborhood watch,’ the technology captures and stores video from millions of households and sweeps up footage of countless bystanders who may be unaware that they are being filmed,” Markey said in a statement. “I am particularly alarmed to learn that Ring is pursuing facial-recognition technology with the potential to flag certain individuals as suspicious based on their biometric information.”

Until very recently, Ring would not disclose how many of these partnerships it currently has. Following media pressure, however, the company said in late August it had 405 active agreements.

## A growing list of concerns

Throughout the summer, reports from outlets including The Washington Post, Gizmodo, CNET, and Vice Motherboard have dug into the details of these agreements, which are rarely made public. The reports have found that Ring writes the press releases, social media posts, and talking points police departments use to encourage widespread Ring adoption. The company also asks police not to call its surveillance products

“security cameras” or use the word “surveillance.”

Concerns also abound about user privacy. Ring claims not to share lists of users or give maps pinpointing exact locations of cameras to police. In August, the company told Ars that participating agencies “must go through the Ring team when making a video request to customers,” adding, “Customers can choose to opt out or decline any request, and law enforcement agencies have no visibility into which customers have received a request and which have opted out or declined.”

But multiple reports have found evidence that Ring shared maps featuring active cameras with police in 2018, basically as a sales tactic to convince a police department to sign up for the partnership program by demonstrating how many cameras were already operating in its jurisdiction. Reports also found evidence that Ring collected data about purchasers which it then shared with police in order to cross-reference eligibility for subsidy programs or camera giveaways that police conduct, in partnership with Ring.

The company also gets access to 911 call data in some jurisdictions, which it uses to “curate” crime news for its Neighbors app. The app, while open to anyone, is optimized for Ring users, who can easily share footage from their doorbells through it. Police can also use their companion portal to send out a localized blast to Neighbors users requesting footage as part of an investigation. Although Ring now says it does not share data about users who decline to share their footage, at one point it gave cops a breakdown about how their requests were performing.

Late last year, the ACLU also flagged a patent application from Ring that would allow devices to ship with facial-recognition software, such as Amazon’s controversial Rekognition system. The patent would allow police or homeowners to flag certain faces as “suspicious.” If a suspicious face showed up on camera, police could then be

dispatched to its location. Rekognition, however, is far from reliable and, like many other facial recognition services, is particularly likely to indicate false positives for people of color.

## Clear answers?

Sen. Markey gave Ring until September 26 to answer questions that reporters and the general public have increasingly been trying to gain clarity on. Those inquiries relate not only to information requests but also to data retention and sharing policies, as well as other privacy concerns.

“How long has Ring prompted its users to share video footage with law enforcement?” Markey asked Ring, pushing for a “detailed timeline of when this sharing began and how, if at all, Ring has changed its policies” over time.

The letter asks Amazon to provide a list of all law enforcement agencies that have ever had or currently have access to Ring video, as well as a copy of a standard sharing agreement. It also asks if Ring requires police departments to delete users’ footage after a certain period, if Ring requires police departments to handle footage in such a way as to minimize the risk of data breaches or leaks, and if Ring has any kind of language in those agreements either permitting or barring police from sharing footage they obtain with third parties.

Sen. Markey also expressed strong concern about the potential for Ring products to contribute to racial profiling and civil liberties violations, especially if Rekognition integration does become a feature. He asked the company to provide a timeline for when or if it plans to add such features as well as a list of criminal justice and civil liberties consultants it has consulted in its work.

https://arstechnica.com/?p=1562925

# DOE has decided many lightbulbs don’t have to meet efficiency standards

## reader comments

279 with 137 posters participating, including story author

## Share this story

Among the stranger subjects that has been caught up in the political wars raging in the United States is the lowly lightbulb. Back in the George W. Bush administration, a law was passed that set efficiency standards for a variety of lightbulbs and allowed the Department of Energy (DOE) to expand the standards going forward.

Almost immediately afterward, legislators who apparently find efficiency a threat to the American way of life had second thoughts, and they started undermining the law’s implementation. As a result, the first real evaluation and update of the standards didn’t take place until late in Obama’s second term. Now, the Trump administration has officially thrown out the results of the work done by Obama’s DOE and has issued a rule that prevents the standards from applying to a variety of bulbs.

# How in the world did we get here?

So how did lightbulbs become a political controversy? Back during the second Bush administration, bulbs were an obvious target for efficiency measures, given how poorly incandescents do on those measures and due to the fact that there were promising newer technologies—compact fluorescents and LEDs—that hadn't really put a dent in the incandescent markets. And, while individual electricity savings would be small, nationwide standards would ensure that the overall savings could be substantial. Increased efficiency on that scale has been a contributing factor to the United States' ability to lower its total electricity use even as its economy has expanded.

As a result, lightbulb efficiency standards were written into the Energy Independence and Security Act, passed into law in 2007. Unlike many laws that become controversial, this one was remarkably reasonable. It set efficiency standards through a very simple measure: how many lumens of light were produced per Watt of power. It focused initial standards on the bulbs with the largest percentage of the market: standard-sized screw-ins for lamps and fixtures. It also included mechanisms for reevaluating the standards and expanding them to additional types of bulbs as more efficient technology matured. Finally, the act recognized that incandescent manufacturers might find design loopholes that let them avoid the standards, so it gave the DOE the right to extend the standards to new types of bulbs.

Within a few years, however, the law had ended up stirring a public controversy. Part of this is the idea that a law banning incandescent lightbulbs fed into the conservative narrative of government overreach and intrusion. (Technically, incandescents would be allowed if they could be made to meet the standards, a subtlety that was often ignored.) And part of it seems to be the general attitude among conservatives that

anything environmentally friendly is good for their political opponents and has to be resisted (“wrecking the planet to own the libs” appears like it may be a thing).

As a result, riders were attached to budget bills for several years that prevented the DOE from spending any money to evaluate lightbulb efficiency standards. By the time budget deals eliminated these riders, we were into Obama’s second term. The DOE didn’t complete its evaluation until 2017. At the time, the law seems to have been effective: LED bulbs had come down dramatically in price, and the ability to manufacture them at large scales was well established. As a result, the DOE issued a rule that would extend the standards to a variety of additional bulb types that had not originally been targeted.

## That was then, this is now

As with most regulations generated by the Obama administration, the 2017 DOE rule on lightbulb efficiency was targeted by the Trump administration. After proposing a rule and soliciting public comment on it, the new rule was issued yesterday. It essentially undoes everything decided by the Obama administration.

The 2017 rules had required a number of additional lighting types to meet efficiency standards, including three-way bulbs, various types of bulbs used in construction and industrial settings, smaller bulbs such as those used in candelabra-style fixtures, and high-output lamps. With the new rules issued by the Trump administration, none of these would be regulated.

In doing so, the administration is specifically following the wishes of various lightbulb manufacturers, who presumably still have viable production facilities dedicated to churning out incandescents. Opposing the changes were a collection of state attorneys general, environmental organizations, and a few electrical utilities. The latter are from California,

which has set aggressive renewable production targets that will be easier to hit if electricity usage continues to drop.

The DOE's logic in supporting this decision can be a bit tough to follow. Even though the DOE followed the law and re-evaluated the efficiency standards, the DOE claims that its secretary never made the official determination that the standards needed to be amended. In the absence of that determination, there's no requirement that it modify the standards by any specific date—even though the standards had already been modified.

Separately, the groups objecting to this decision note that the law indicates that the DOE shouldn't drop any efficiency standards below 45 lumens/Watt. By excluding these bulbs, they argue, the DOE is essentially setting the standard to zero. But the DOE counters that by saying it's only determining if the bulbs are subject to standards, not actually setting any.

## Lawsuits on the way

The law seemingly anticipated these sorts of impasses by directing the DOE to establish standards for any bulbs that end up being used as general lighting; this would, for example, allow the DOE to start regulating different bulb formats if manufacturers started selling them as replacements for a regulated format. But in its new rule, the DOE is specifically disavowing that authority, writing: "It is unlikely Congress intended that DOE have broad discretion to regulate an incandescent lamp out of existence based on an assumption that manufacturers could make and sell an LED version of the lamp."

As a result, the DOE has declared that it will be ignoring its authority to use "convenient unregulated alternatives" as a standard to identify things that need to be regulated.

The last few paragraphs could possibly be summarized as "there

are many things here that will end up getting the DOE sued.” And, given the list of organizations that opposed these changes, including a large number of states, that’s almost certain to happen.

But it’s worth taking a step back and looking at the big picture again. The original legislation appears to have been well-designed and successful: LED bulbs are now inexpensive, abundant, and remain long-lived and efficient. And yet, due to lingering animosity toward the existence of any standards at all, the Trump administration is doing its best to keep the legislation from being used to regulate the hardware it was obviously intended for.

The full text of the DOE’s decision is available here.

https://arstechnica.com/?p=1562961

---

# IoT botnet creator cops plea to hacking more than 800,000 devices

Getty Images | Marilyn Nieves

## reader comments

14 with 13 posters participating

## Share this story

A 21-year-old Washington man has pleaded guilty to creating botnets that converted hundreds of thousands of routers, cameras, and other Internet-facing devices into money-making denial-of-service fleets that could knock out entire Web hosting companies.

Kenneth Currin Schuchman of Vancouver, Washington, admitted in federal court documents on Tuesday that he and two other co-conspirators operated Sartori and at least two other botnets that collectively enslaved more than 800,000 Internet-of-Things devices. They then used those botnets to sell denial-of-service attacks that customers could order. Last October, while on supervisory release after being indicted for those crimes, Schuchman created a new botnet and also arranged a swatting attack on one of his co-conspirators, the plea agreement, which is signed by the hacker, said.

The crime outlined in the court documents started with the advent in late 2016 of Mirai, a botnet that changed the DDoS paradigm by capitalizing on two salient features of IoT devices: their sheer numbers and their notoriously bad security. Mirai scanned the Internet for devices that were protected by an easy-to-guess default password. When the botnet found one, it corralled it into a botnet that could overwhelm even large targets with more junk traffic than they could handle.

Within a few weeks, Mirai was producing record-setting DDoS attacks, one of which took out security site KrebsOnSecurity for days. In short order, the Mirai source code was openly published in an act that made it easy to spin up DIY clones of Mirai.

Schuchman used the Mirai source code to create a new botnet that quickly infected 100,000 routers. Schuchman, the plea deal said, bragged that the botnet allowed him and his co-

conspirators to compromise 32,000 devices belonging to a large Canadian ISP, a feat he claimed allowed him to DDoS targets with bandwidth of an astounding 1 terabit per second. The secret to its success: Sartori, as the botnet was christened, exploited security vulnerabilities—some of which were zero-days—in infected devices, even when they were protected by strong passwords.

According to Tuesday's plea deal, Schuchman used the monikers "Nexus" and "NexusZeta" to converse with co-conspirators using the handles Vamp and Drake. The trio's goal was to improve upon Satori and build their own DDoS franchise. The results were Okiru, which exploited vulnerabilities in the Goahead family of surveillance cameras, and Masuta, which infected as many as 700,000 nodes by exploiting vulnerable Huawei and Gigabit Passive Optical Network (GPON) fiber-optic networking devices.

The plea agreement stated:

> *Logs during the Masuta time period depict a large number of attacks launched at the end of November by SCHUCHMAN, Drake, and others, including paying customers of the criminal botnet scheme. At this time, SCHUCHMAN also operated his own distinct DDoS botnet which he utilized to attack IP addresses associated with ProxyPipe. At the same time, SCHUCHMAN was also actively scanning the internet for vulnerable telnet devices for the purpose of identifying additional devices to incorporate into his active botnets. When SCHUCHMAN received abuse complaints related to the scanning, he responded in his father's identity. SCHUCHMAN frequently used identification devices belonging to his father to further the criminal scheme.*

It wasn't hard for authorities to track down the real-world identity tied to Nexus and NexusZeta. He was indicted last August, but even then, his criminal conduct didn't end. The

plea agreement states:

> *SCHUCHMAN went so far as to create a new Qbot DDoS botnet variant on or about October 2018 while on supervised release after having been charged by indictment with creating and deploying DDoS botnets. SCHUCHMAN also used information gleaned from discovery in this matter to identify the whereabouts of his co-conspirator Drake for the purpose of facilitating a "swatting" attack that involved a fake 911 call alleging a hostage incident at Drake's residence, triggering a substantial law enforcement response in October 2018.*

Schuchman pleaded guilty to one count of aiding and abetting computer intrusions. He faces a maximum penalty of 10 years in prison and $250,000 in fines, but the recommended sentence agreed to by prosecutors calls for penalties "at the low end of the guideline range." The Daily Beast reports that Schuchman has Asperger's syndrome, a condition that may also influence the judge hearing his case. Schuchman's sentencing hearing is scheduled for November.

https://arstechnica.com/?p=1562271