Richard Stallman leaves MIT after controversial remarks on rape

Enlarge / Richard Stallman in 2015.
Michael Debets/Pacific Press/LightRocket via Getty Images

reader comments

114 with 61 posters participating, including story author

Share this story

Free software pioneer Richard Stallman has resigned from his posts at MIT and the Free Software Foundation after leaked emails showed him quibbling over the definition of rape in a conversation related to Jeffrey Epstein.

The conversation that triggered Stallman's fall started when someone—names other than Stallman's are redacted in the leaked emails—posted about a planned protest at MIT. The email stated that famed MIT computer scientist Marvin Minsky "is accused of assaulting one of Epstein's victims."

Stallman objected, saying that the blurb "does an injustice" to Minsky because even if it's true that the then-17-year-old had sex with Minsky, "the most plausible scenario is that she presented herself to him as entirely willing." (One witness to the alleged incident says that Minsky, who died in 2016, declined to have sex with her.)

Someone pointed out that the age of consent in the US Virgin Islands, where the incident allegedly occurred, is 18. That makes sex with a 17-year-old girl, "willing" or not, statutory

rape. But Stallman wasn’t persuaded.

“I think it is morally absurd to define ‘rape’ in a way that depends on minor details such as which country it was in or whether the victim was 18 years old or 17,” Stallman wrote.

Stallman has always been a stubborn nonconformist

Enlarge / Stallman speaks at a conference in 2014.

Stallman has long been famous for his extreme devotion to the cause of free software. He spearheaded the GNU project to produce a Unix-like operating system that would be free for anyone to use and modify. GNU software became a key part of the operating system most people today call Linux—to the immense irritation of Stallman, who believes the GNU components are significant enough that the package should be called GNU/Linux.

Also significant was Stallman's philosophical, political, and legal work on behalf of free software. Stallman founded the Free Software Foundation in 1985 to advocate against the spread of proprietary software. By 1989, he had drafted the GNU General Public License, a "copyleft" software license that guarantees users the freedom to modify software as long as they share any resulting code under the same license.

For decades, Richard Stallman has traveled the world extolling the benefits of free software. Before he travels to give a speech, he frequently sends event hosts a lengthy email describing his conditions.

Stallman is legendary for his stubbornness and ideological inflexibility. Event organizers seeking to host Stallman are banned from using the terms "Linux" or "open source"—a term he views as a deliberate rejection of the moral stance implied by the term "free software."

Stallman also makes a number of suggestions that have nothing to do with politics or software.

"If you can find a host for me that has a friendly parrot, I will be very very glad," Stallman wrote in a 2012 edition of the email. However, he asked hosts not to purchase a parrot for his benefit.

"If you buy a captured wild parrot, you will promote a cruel and devastating practice, and the parrot will be emotionally scarred before you get it," he wrote.

For decades, Stallman has refused to use any proprietary software, which has meant opting out of many contemporary technology products. If organizers want to stream his speech, they must arrange to do so using entirely free software—a nontrivial challenge in a world where so much video streaming software is proprietary.

That stubbornness was on display in the email thread that caused Stallman's downfall at MIT. At one point, someone linked to a deposition given by one of Epstein's victims.

"I visited that URL and got a blank window," Stallman wrote. "It is on Google Drive, which demands running nonfree software in order to see it." He asked someone else to download the file and send him the part relating to Minsky.

Stallman's past statements stoked further outrage

Former Free Software Foundation President Richard Stallman. When Stallman's emails were published, it caused an uproar at MIT, in the free software community, and on the broader Internet.

People began digging into Stallman's past writings and found other controversial comments. "I think that everyone age 14 or above ought to take part in sex, though not indiscriminately," Stallman wrote in a 2003 post about the UK banning minors from having access to sexually explicit material. "Some people are ready earlier."

"It is unnatural for humans to abstain from sex past puberty, and while I wouldn't try to pressure anyone to participate, I certainly encourage everyone to do so," he added.

In 2011, he criticized laws against child pornography. "'Child pornography' might be a photo of yourself or your lover that the two of you shared," he wrote. "It might be an image of a sexually mature teenager that any normal adult would find

attractive. What's heinous about having such a photo?"

"Even when it is uncontroversial to call the subject depicted a "child", that is no excuse for censorship," he added. "Having a photo or drawing does not hurt anyone, so and if you or I think it is disgusting, that is no excuse for censorship."

In the last week, after his comments received widespread attention, Stallman said he was rethinking some of these views.

"Many years ago I posted that I could not see anything wrong about sex between an adult and a child, if the child accepted it," he wrote on Saturday. "Through personal conversations in recent years, I've learned to understand how sex with a child can harm her psychologically. This changed my mind about the matter: I think adults should not do that."

In another post later the same day, Stallman objected to headlines saying he defended Jeffrey Epstein.

"Headlines say that I defended Epstein," Stallman wrote. "Nothing could be further from the truth. I've called him a 'serial rapist,' and said he deserved to be imprisoned. But many people now believe I defended him—and other inaccurate claims—and feel a real hurt because of what they believe I said."

"I'm sorry for that hurt," Stallman added. "I wish I could have prevented the misunderstanding."

On Monday, Stallman resigned from MIT "due to pressure on MIT and me over a series of misunderstandings and mischaracterizations." He also resigned as president of the Free Software Foundation.

https://arstechnica.com/?p=1569379

Instigator of fatal Kansas swatting receives prison sentence

Enlarge / A police SWAT Team at work.

reader comments

170 with 78 posters participating

Share this story

The teenager who arranged for someone else to phone in a prank police call that resulted in a man’s death is going to prison.

Casey Viner, now 19, will serve 15 months in prison and pay $2,500 restitution, the US District Attorney for Kansas said. After release, Viner will also be barred from online gaming for a period of two years.

Viner admitted in court that in 2017 he argued with a co-defendant, Shane Gaskill, while playing *Call of Duty* online. He then contacted a third person, Tyler Barriss, and asked him to swat Gaskill. Viner, however, had an incorrect address for Gaskill, and Barriss instead sent a swat team to the house of 28-year-old Andrew Finch, who was then shot and killed by police.

Viner also tried to erase records on his phone of his communications with Gaskill following the event. He pleaded guilty to one count of conspiracy and one count of obstructing

justice. (Gaskill struck a deal with prosecutors for deferred prosecution, and charges against him may ultimately be dropped.)

Barriss in March was sentenced to a 20-year prison term following his guilty plea for 50 felonies relating to his role in dozens of swatting crimes, for which he showed little remorse.

“Swatting, and soliciting others to swat someone, are more than foolish,” said US Attorney Stephen McAllister. “Such actions are reckless, dangerous and, as this case proves, potentially tragic. Swatting is not a prank, and it is no way to resolve disputes among gamers. Once again, I call upon gamers to self-police their community to ensure that the practice of swatting is ended once and for all.”

https://arstechnica.com/?p=1569385

The fight over fuel economy rules is getting messy

Getty Images

reader comments

48 with 23 posters participating

Share this story

Legal wrangling among the federal government, the state of

California, and four automakers who—oddly—are asking for more stringent regulations got even more knotty this month, when the Department of Justice reportedly launched an antitrust probe into companies that struck a deal with California climate regulators.

Now some members of Congress are urging an independent investigation of the investigation, amid suspicions that the probe is an attempt to punish the automakers—and California—for parting ways with federal policy on fuel economy.

The "what' is confusing; the "why," less so. If the average global temperature rises by 4°C by the end of the century, as it may be on track to do, scientists say a whole bunch of bad things would likely happen: higher sea levels, more extreme weather. In the US, transportation is responsible for 29% of greenhouse gas emissions, and nearly 60% of those come from light-duty vehicles like passenger cars.

That's why the Obama administration decided in 2012 to (slowly) strengthen regulations governing vehicles' tailpipe emissions and fuel economy standards, requiring each automaker's fleet to average 54.5 miles per gallon by 2025 and boosting the penalty for missing that target. The Trump administration, on the other hand, wants to freeze those standards at 37mpg and delay the penalty hike, arguing that it will save automakers money, keeping prices low so that more people can buy newer cars with safer technology. (Electric vehicle proponents have questioned this logic.)

California has other ideas. In July, state regulators said they had reached their own deal with Ford, Honda, BMW, and Volkswagen, which would continue to ramp up fuel economy standards through 2025. Together, the four automakers account for roughly 30% of US car sales. The compromise would reach the same average fuel economy levels as the Obama-era standards but with a slighter longer timeline.

California is a vital market for automakers, and not just because it's the nation's largest economy: thirteen other states have pledged to follow its lead on emissions rules. Together, those 14 states account for about one-third of US vehicle sales. One set of rules for one-third of the car-buying country, and another for the rest would be disastrous for carmakers.

Other big automakers are in wait-and-see mode. General Motors reportedly believes the California deal doesn't give manufacturers enough credit for investments in fully electric vehicles. The Automobile Alliance, which represents the four carmakers involved in the California deal but also non-signatories like GM and Fiat Chrysler, says its priority is avoiding "uncertainty from protracted litigation."

California is able to set its own emissions standards thanks to text in the Clean Air Act that dates back to the 1970s. At that time, California was well ahead of the rest of the country in combating emissions, so Congress gave it authority to write its own, stricter rules. The Bush administration tried to deny California's effort to set its own emissions standards in 2007, but Obama had taken office before the case was resolved.

Now the Trump administration wants to revoke California's legal authority to set its own rules, and it's trying to do that through lawsuits and new regulations. (Technically, California and other states sued *it*, arguing that it doesn't have the authority to nix the Obama-era rules.) Legal experts say the administration may have a tough road ahead without Congress' help. "The statute is very clear: It says EPA shall grant the waiver," Cara Horowitz, co-executive director of the Emmett Institute on Climate Change and the Environment at UCLA School of Law, has told WIRED. However, federal judges at a

hearing in Washington, DC, earlier this month signaled they would be willing to consider the merits of the administration's arguments.

Experts say the antitrust probe into California's dealings is unusual and that antitrust charges might not apply to businesses' cooperative agreements with government entities—the state of California, for example. Congress could also choose to intercede to prevent the federal government from using antitrust laws as punitive sticks.

Congress, meanwhile, may launch an investigation into the antitrust probe. In a Friday letter to the head of the Department of Justice's Office of the Inspector General, Senate Judiciary Committee member (and presidential candidate) Kamala Harris (D-California) urged the office to examine the motivations for the probe, calling it part of a "multi-pronged assault on California's framework." The House's Judiciary Committee, meanwhile, which is controlled by Democrats, has said that it will seek documents and hearings connected to the antitrust investigation.

California politicians also seem ready for a long-haul flight. "The Trump administration has been attempting and failing to bully car companies for months now," California Governor Gavin Newsom said in a statement earlier this month. "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."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1568673

Meet the three North Korean hacking groups funding the country’s weapons programs

Enlarge / Hacking for their home country, we guess.

reader comments

37 with 32 posters participating

Share this story

The Trump administration is sanctioning three North Korean hacking groups widely accused of carrying out attacks that targeted critical infrastructure and stole millions of dollars from banks in cryptocurrency exchanges, in part so the country could finance its weapons and missiles programs.

All three of the groups are controlled by North Korea’s primary intelligence agency, the Reconnaissance General Bureau, or RGB, officials with the US Department of Treasury said in a statement published on Friday. Collectively, the groups are behind a host of cyber attacks designed to spy on adversaries and generate revenue for nuclear weapons and ballistic missile programs.

“Treasury is taking action against North Korean hacking groups that have been perpetrating cyber attacks to support illicit weapon and missile programs,” Sigal Mandelker, Treasury under-secretary for terrorism and financial intelligence, said in Friday’s statement. “We will continue to enforce existing US and UN sanctions against North Korea and work with the international community to improve cybersecurity of financial

networks.”

The best-known of the three sanctioned groups is Lazarus, the name given to a team created as early as 2007 that targets militaries, governments, and companies in the financial, manufacturing, publishing, media, entertainment and shipping industries. The FBI tied Lazarus to the 2014 hack of Sony Pictures that destroyed data on thousands of company computers and published embarrassing emails from company executives to avenge a film that depicted the assassination of North Korea’s leader.

But the best-known work widely attributed to Lazarus was the WannaCry ransom worm outbreak in 2017. The malware used a Windows exploit developed by and later stolen from the National Security Agency that allowed the worm to spread rapidly from computer to computer with no user interaction.

Within hours, WannaCry had spread to 150 countries and shut down an estimated 300,000 computers. Hospitals in the UK were hit particularly hard, leading to the cancellation of more than 19,000 appointments and costing the country’s National Health Service more than $112 million.

The new sanctions also apply to two Lazarus subgroups. The first is known as Bluenoroff, which was formed as a means to earn revenue in the wake of increased global sanctions against the North Korean government. This is the group that was behind a 2016 hack on a Bangladesh central bank that almost got away with stealing $851 million. A typographical error prevented the illicit transaction from going through, but the attackers still made off with $81 million. Bluenoroff has also carried out successful hacks against banks in India, Mexico, Pakistan, the Philippines, South Korea, Taiwan, Turkey, Chile, and Vietnam.

Security firms including Symantec and FireEye have chronicled the work of this Lazarus subgroup as it systematically

exploited weaknesses in the SWIFT payment network used by banks around the world. The name Bluenoroff was coined in 2017 by researchers from Kaspersky Lab, who were the first to attribute the group as a standalone subunit of Lazarus. The group's name was based on a tool it used called "nroff_b.exe."

Enlarge / The tool called nroff_b.exe is highlighted in red.
The other Lazarus subgroup is known as "Andariel." It focuses on hacks targeting foreign businesses, financial services, and government agencies. Security companies first noticed Adariel around 2015 when it hit targets in South Korea. The team has been responsible for attempts to steal bank card information by hacking into ATM networks to withdraw cash or steal data that could be sold to other criminals. The group, which was discovered by South Korea's Internet and Security Agency, or Kisa, is also responsible for developing malware to hack online poker and gambling sites.

Trend Micro has a useful breakdown of the three North Korean hacking groups here.

Friday's statement said North Korean hacking operations have also targeted virtual asset providers and cryptocurrency exchanges, possibly in an attempt to obfuscate revenue streams

used to support the countries weapons programs. The statement also cited industry reports saying that the three North Korean groups likely stole about $571 million in cryptocurrency from five exchanges in Asia between January 2017 and September 2018. News agencies including Reuters have cited a United Nations report from last month that estimated North Korean hacking has generated $2 billion for the country's weapons of mass destruction programs.

It's not clear how a new round of sanctions will affect an impoverished nation that is already ostracized by most of the world. And if the UN's $2 billion estimate is correct, it's hard to think Friday's move will have any practical effect.

https://arstechnica.com/?p=1568689

Congress wants Facebook, Google, Apple, and Amazon emails as probe heats up

Enlarge / The dome of the United State Capitol Building in Washington, DC.
Getty Images | Phil Roeder

reader comments

58 with 43 posters participating, including story author

Share this story

The long summer recess for Congress is at last well and truly over. The House Judiciary Committee has ramped up for the fall season, issuing demands for huge piles of documentation from Apple, Amazon, Facebook, and Google as its antitrust probe into Big Tech grows.

The committee launched the bipartisan inquiry in June, seeking in part to determine "whether existing laws are adequate" to the task of regulating the sprawling tech titans that power the 21st century economy. As part of that probe, the committee has now issued lengthy requests for information to the four companies digging deeply into the question of competition.

The tech sector is facing scrutiny from all sides at the moment. The House investigation is separate and distinct from the various antitrust probes against the same four companies the Federal Trade Commission, the Department of Justice, and nearly all the states currently have in progress.

"There is growing evidence that a handful of corporations have come to capture an outsized share of online commerce and communications," committee chairman Jerrold Nadler (D-N.Y.) said in a written statement. The responses should give the committee a "better understanding" of how much market power the companies have, he added, "how they are using that market power, whether they are using their market power in ways that have harmed consumers and competition, and how Congress should respond."

An antitrust probe is not simply an examination of whether a company is a monopoly. Being the dominant player in a market is not against the law. Esven in a highly competitive environment, someone, at any given time, is going to be ahead.

Rather, the probes are looking for evidence of anticompetitive behavior: tactics that keep you at the top of the heap unfairly, or underhanded strategies that you use to knock out

potential competitors before they can become a threat. Critics of Facebook, for example, allege that the company buys up startups that might eventually compete with it and then either integrates those companies' products or winds them down. Apple likewise uses data from App Store sales to choose what kind of apps and features it should develop in-house, and Amazon faces an antitrust probe in Europe over the way it competes against third-party marketplace merchants using its platform.

Sprawling empires

The extensive lists of questions posed to the four companies could generate some fascinating results. On their own, the letters already make very clear how massive and sprawling a footprint many of these companies have—they also make clear the implication that competitors are at best trying to scramble around the four metaphorical eight-ton gorillas sitting on the field.

For example, each of the four companies is asked to provide a list of the top 10 competitors to several of its services, including an explanation of *why* each entity on the list constitutes competition. Coming up with 10 viable competitors to the core Facebook app, which boasts 244 million users in the US and Canada and 2.4 billion worldwide, may prove challenging even for Facebook's experienced executives. From an outsider's vantage point, meanwhile, the top competition to Facebook Messenger may include services such as WhatsApp—which Facebook has owned since 2014.

The committee also requests access to more than 10 years' worth of communications to or from top executives at all four firms, regarding dozens of topics each. The list to Amazon, for example, includes questions about Amazon Web Services, the company's third-party retail marketplace, consumer data, contract agreements, sorting and ranking algorithms, Amazon Prime, and several other matters.

All the companies are also asked to provide communications relating to any cases filed in the US relating to allegations of anticompetitive behavior within the past 10 years, as well as relating to "any prior investigation or litigation involving a US or foreign government entity, including US state attorneys general offices, within the past 10 years" relating to allegations that the company "engaged in anticompetitive practices or otherwise violated antitrust laws." Those communications alone will likely generate untold reams of data in response, as the companies are not only facing current US antitrust investigations; they've also faced previous probes both in their home country and elsewhere.

For example, the FTC has been contemplating antitrust action against Google for the better part of a decade. In 2012, an internal memo circulated to all five commissioners that strongly recommended launching an antitrust suit against Google for abusing its dominance, although the commission ultimately decided in 2013 not to bring charges.

The European Union, meanwhile, has fined Google billions of dollars for antitrust violations just in the past three years. In 2017 it was a €2.42 billion fine for the company steering shoppers toward Google's platform in search results, in 2018 it was a €4.34 billion fine for the company unfairly pushing its own apps ahead of competitors', and earlier this year two fines were joined by another €1.5 billion fine for the company abusing its dominant position in the ad sales market. (For conversion's sake, €1 billion there is roughly $1.11 billion here.)

The committee gave all four companies a deadline of October 14 to comply with the requests for information. You can read the full text of the four letters here: Amazon (PDF), Apple (PDF), Facebook (PDF), and Google (PDF).

https://arstechnica.com/?p=1568357

Check the scope: Pen-testers nabbed, jailed in Iowa courthouse break-in attempt

Enlarge / The Dallas County, Iowa courthouse, the site of a penetration test gone spectacularly wrong.

reader comments

166 with 92 posters participating, including story author

Share this story

Two security contractors were arrested in Adel, Iowa on September 11 as they attempted to gain access to the Dallas County Courthouse. The two are employees of Coalfire—a "cybersecurity advisor" firm based in Westminster, Colorado that frequently does security assessments for federal agencies, state and local governments, and corporate clients. They claimed to be conducting a penetration test to determine how vulnerable county court records were and to measure law enforcement's response to a break-in.

Unfortunately, the Iowa state court officials who ordered the test never told county officials about it—and evidently no one anticipated that a physical break-in would be part of the test. For now, the penetration testers remain in jail. In a statement issued yesterday, state officials apologized to Dallas County, citing confusion over just what Coalfire was going to test:

> *State court administration (SCA) is aware of the arrests made at the Dallas County Courthouse early in the morning on September 11, 2019. The two men arrested work for a company hired by SCA to test the security of the court's electronic records. The company was asked to attempt unauthorized access to court records through various means to learn of any potential vulnerabilities. SCA did not intend, or anticipate, those efforts to include the forced entry into a building. SCA apologizes to the Dallas County Board of Supervisors and law enforcement and will fully cooperate with the Dallas County Sheriff's Office and Dallas County Attorney as they pursue this investigation. Protecting the personal information contained in court documents is of paramount importance to SCA and the penetration test is one of many measures used to ensure electronic court documents are secure.*

The case is an example of the legal risks faced by security testing firms, particularly when the scope of such tests is vague. Even the most basic electronic security tests, when done outside of the bounds of a contractual agreement, could land the testers in trouble, as Ars reported when Gizmodo reporters attempted to phish Trump administration and campaign figures in 2017.

Josh Rosenblatt, a Maryland attorney who teaches at the University of Baltimore and is a legal instructor for the Baltimore Police Department, noted the legal complications of penetration testing in a presentation at BSides Charm. "If you have a full black-box assessment," Rosenblatt said—meaning a security assessment with no scope set and only vague definitions of how the security is to be checked—"you might run into issues." That's particularly the case when the organization issuing the assignment doesn't own the infrastructure being tested.

"The scope is everything," Roseblatt explained. If the scope

is only vaguely defined, “you could find yourself exposed to legal liability.”

Coalfire’s Justin Wynn and Gary Demercurio, who are still in jail [**Update**: They appear to have made bail on Thursday], have been charged with third-degree burglary and possession of burglary tools. Their bond has been set at $50,000, and they are scheduled to appear for a preliminary hearing on September 23—in the same courthouse they were caught breaking into.

https://arstechnica.com/?p=1568353

Forwarding email is a crime, Jerry Falwell Jr. says after leaks to media

Enlarge / Liberty University President Jerry Falwell Jr. participates in a town hall meeting in March 2019.

reader comments

288 with 131 posters participating

Share this story

High-profile evangelical conservative Jerry Falwell Jr., a staunch Trump supporter and president of Liberty University, wants the FBI to investigate current and former university employees for… forwarding emails.

Falwell claims to have evidence that employees “improperly shared” emails belonging to the university, the Associated Press reports. Falwell said the communications were shared as part of a “criminal” smear campaign and “attempted coup.”

Falwell told the AP he contacted the FBI before the story was published, when he learned reporters were reaching out to Liberty employees about the “stolen” emails. “I am going to the authorities and I am going to civil court” over the shared documents, Falwell said.

The emails in question form the cornerstone of a magazine feature Politico ran Monday on Falwell and Liberty University. The story, running under the headline “Someone’s gotta tell the freaking truth,” dug into financial arrangements between the Falwell family, the school, and other entities, and it depicted the university as a “dictatorship” under Falwell’s thumb.

One official at Liberty told Politico, “We’re not a school; we’re a real estate hedge fund.” Politico added that several other employees:

> *[D]etailed other instances of Falwell’s behavior that they see as falling short of the standard of conduct they expect from conservative Christian leaders, from partying at nightclubs, to graphically discussing his sex life with employees, to electioneering that makes uneasy even those who fondly remember the heyday of the late Rev. Jerry Falwell Sr., the school’s founder and Falwell Jr.’s father, and his Moral Majority.*

Reuters this week also published a selection of emails in which Falwell used insulting or disparaging language to describe Liberty University students, staff, and parents to other administrators.

“I’m not going to dignify the lies that were reported

yesterday with a response," Falwell told the AP, but he said he hired "the meanest lawyer in New York" to pursue civil cases against sources who shared communication with Politico.

"Liberty owns every single one of those emails. It's our property. They were working for us when they used our server," Falwell told the AP. "Our policies make it clear every email sent on our server is owned by Liberty, and if anybody shares it with anybody outside Liberty, it is theft. And so that's the underlying crime."

Employees who spoke with Politico apparently anticipated this kind of response from Falwell:

> *"Everybody is scared for their life. Everybody walks around in fear," said a current university employee who agreed to speak for this article only after purchasing a burner phone, fearing that Falwell was monitoring their communications. The fear is not limited to Liberty's campus. Several people who lack any tie to Liberty but live in the school's hometown of Lynchburg, Virginia, refused to go on the record for this story, fearing Falwell would take revenge upon them and their families. "Fear is probably his most powerful weapon," a former senior university official said.*

Against the rules, but not the law

Politico reported that many Liberty University employees and board members are required to sign nondisclosure agreements that bar them from openly discussing matters pertaining to the school or to Falwell. Those agreements may be enforceable against the folks who talked to Politico, or they may not; that can be argued out in civil court.

The Computer Fraud and Abuse Act (CFAA) is the big law that governs what is and isn't computer fraud. The CFAA outlines criminal penalties for an array of computer crimes, such as

breaking into a computer or system to steal national security secrets, financial data, or to commit extortion. It also contains provisions relating to, for example, intentionally transmitting viruses, or trafficking in passwords.

So hacking a computer or system to obtain someone else's emails is a crime. But choosing of your own volition to share an email in your possession is not, unless the content in it would violate some other kind of law, such as an executive sharing insider financial information in violation of securities law, a doctor sharing medical information in violation of HIPAA, or a lawyer sharing confidential information in violation of client privilege.

Some legal experts have made the case that email can be subject to copyright protection. Even if Liberty were to pursue a copyright claim against the sources who provided documents to Politico, though, that would be a different kind of claim from Falwell's assertion that employees stole Liberty property off of Liberty servers by sharing copies of emails.

Falwell's assertions of theft seem unlikely to be greeted with a strong response from the FBI, according to an expert the AP spoke with. He called Falwell's assertions "totally insane," adding, "I don't think any law enforcement agency is going to be interested in this one."

https://arstechnica.com/?p=1567915

California passes bill that

threatens Uber and Lyft’s business model

Enlarge / California Governor Gavin Newsom.
Ray Chavez/The Mercury News via Getty Images

reader comments

194 with 80 posters participating, including story author

Share this story

Both houses of California’s legislature have passed sweeping legislation requiring businesses to treat more of their workers as employees rather than independent contractors. As a result, more workers will enjoy protections like the minimum wage and benefits such as unemployment insurance. The bill is now on its way to Governor Gavin Newsom, who is expected to sign it.

The law will apply across the California economy, but it could have particularly stark consequences for Uber and Lyft—both of which are based in the Golden State. The companies currently treat their drivers as independent contractors, and their entire business model is built around that assumption.

In the hours after the legislation cleared the California legislature, Uber and Lyft both blasted the law and vowed to seek changes.

“California is missing a real opportunity to lead the nation by improving the quality, security and dignity of independent work,” Uber’s Tony West said. In an emailed statement, Lyft argued that the “overwhelming majority of rideshare drivers” want “a thoughtful solution that balances flexibility with an

earnings standard and benefits”—a standard Lyft argues that the new legislation doesn’t meet.

Uber and Lyft are still hoping that Governor Newsom will push through follow-up legislation specifically for “gig economy” workers. If that doesn’t happen, Uber, Lyft, and Doordash have also vowed to spend $30 million backing a ballot initiative to overturn the law.

But if those efforts fail, then “gig economy” companies could be forced to rethink their business models. And the results may not be entirely positive for Uber and Lyft drivers.

More workers will be employees in California

terra24 / Getty

Labor law draws a basic distinction between employees and independent contractors. If you’re an employee, you have a boss who sets your schedule, tells you what kind of work to do, and pays you at least minimum wage. Independent

contractors, on the other hand, are people who—at least theoretically—run their own, separate businesses. Think about a plumber you hire once to fix a leaky pipe, for example.

In recent years, employers have pushed the legal envelope, trying to classify as many workers as possible as independent contractors. Worker rights advocates have objected, arguing that these workers were being wrongfully denied protections they were entitled to under labor law.

One of those conflicts reached the California Supreme Court last year. A same-day delivery company called Dynamex once treated its drivers as employees, but it re-classified them as independent contractors in 2004. Some of those drivers sued, arguing that they should still be considered employees under California law.

Last year the California Supreme Court sided with the drivers, and in the process it established new, broader criteria for determining who was an employee. Under the test, a worker must be treated as an employee unless three conditions are met:

> *(a) The worker is free from control and direction over performance of the work; (b) the work provided is outside the usual course of the business for which the work is performed; and (c) the worker is customarily engaged in an independently established trade, occupation, or business*

This simpler test means that a lot more workers will be classified as employees. But critics worried it could go too far, upending the businesses of professionals who have long operated as independent contractors.

So the California legislature passed legislation to ratify the *Dynamex* ruling while also limiting its scope. It carves out a number of exemptions—largely for high-earning professionals like lawyers, architects, engineers and accountants. People in these skilled occupations often operate their own independent

firms and have significant bargaining power.

Under the new law, photographers, writers, and cartoonists can more easily be independent contractors if they sell fewer than 35 pieces to a single client in a year. If they sell more than that then they're likely to be classified as employees.

Uber, Lyft, Doordash, and other "gig economy" companies lobbied hard for a similar exemption covering their workers, but they came up short. So Uber and Lyft drivers—as well as delivery drivers for other on-demand services—may soon be legally considered employees of these companies.

Uber disputes that. In a Wednesday conference call, Uber chief legal officer Tony West argued that driving a car is "outside the usual course" of Uber's business. "Several previous rulings have found that drivers' work is outside the usual course of Uber's business, which is serving as a technology platform for several different types of digital marketplaces," West said.

For example, a Vermont official accepted that reasoning in a 2017 ruling using a legal standard similar to the one that now applies in California. But it's widely expected that courts in California won't see the issue the same way.

The new law could mean changes for Uber and Lyft drivers

Enlarge / An Uber car.
nycshooter / Getty
A big reason Uber and Lyft have been opposing this bill so ferociously is that their current business model doesn’t fit well into conventional labor law categories.

Conventional labor law assumes that a worker goes to a job, clocks in, works, for a few hours, and then clocks out. In this model, the employer decides what work the worker should do; in exchange the worker is guaranteed to make at least minimum wage. Employers set worker schedules; to protect them, California law guarantees workers overtime pay and mandatory breaks.

By contrast, Uber and Lyft drivers have complete control over where and when they work. In this model, it’s not clear that mandatory overtime pay helps workers, since workers never face pressure from the platforms to work longer hours. If platforms are forced to pay time-and-a-half for overtime hours, they may just ban drivers from working overtime.

A minimum wage guarantee is likely to trigger significant changes to the ride-sharing model. It’s helpful here to look at New York City, where a $17.22 minimum wage for ride-hail drivers went into effect earlier this year.

To make a profit, Lyft needs to make sure drivers bring in at least $17.22 per hour in fares. To accomplish this, Lyft has imposed a new policy that (in the words of Harry Campbell) “prevents drivers from logging on to the company’s app during periods of low demand.” Under the new rules, Lyft drivers in New York “have to wait until ride requests pick up, or drive to a busier neighborhood.”

Whether these changes ultimately benefit drivers is an open question. Probably it will benefit some drivers and harm others. Full-time drivers may not be affected very much, as Lyft exempts its most active drivers from these restrictions. On the other hand, the changes may be bad for part-time drivers who care more about flexible schedules than maximizing earnings.

We can expect similar changes in California if the new legislation ultimately causes drivers to be classified as employees. Companies will likely restrict how many people drive for them and where and when they can work. Workers who are able to get work may enjoy higher earnings, but they’ll lose a bit of autonomy over their schedules. Meanwhile, with fewer drivers on the road, customers may see higher fares and longer wait times.

But the full implications won’t be clear until the new rules make their way through the courts. Uber and Lyft aren’t going to give up their current business model without a fight.

https://arstechnica.com/?p=1567445

Trump demanded retraction after NWS disputed his false hurricane claim

Enlarge / President Donald Trump displaying a doctored forecast map at the White House on September 04, 2019 in Washington, DC.
Getty Images | Chip Somodevilla

reader comments

280 with 134 posters participating

Share this story

The White House pressured the National Oceanic and Atmospheric Administration into backing President Trump over weather forecasters who disputed Trump's incorrect claim that Hurricane Dorian would likely strike Alabama, according to news reports.

"Mick Mulvaney, the acting White House chief of staff, told Wilbur Ross, the commerce secretary, to have the National Oceanic and Atmospheric Administration publicly disavow the forecasters' position that Alabama was not at risk," the New York Times reported today, citing anonymous sources. Ross then warned NOAA "that top employees at the agency could be fired if the situation was not addressed," the Times wrote.

Mulvaney took this action after "President Trump told his staff that the [NOAA] needed to correct a tweet that seemed to

contradict his statement that Hurricane Dorian posed a significant threat to Alabama as of Sept. 1," the Washington Post wrote in an article on the same topic. There are now multiple investigations into whether the NOAA's scientific integrity and independence were undermined.

Trump vs. National Weather Service

On the morning of September 1, Trump tweeted that Alabama "will most likely be hit (much) harder than anticipated."

But the official forecast at the time showed a probable path for the storm center that did not include Alabama at all. The National Weather Service office in Birmingham, Alabama, subsequently tweeted that "Alabama will NOT see any impacts from Dorian" because "the system will remain too far east." (The National Weather Service is part of NOAA.)

Despite that, Trump on September 4 gave a video message and showed a doctored forecast map in which black marker had been used to include Alabama in the hurricane's potential path.

Mulvaney's intervention apparently led to a September 6 statement from NOAA that rebuked the Birmingham National Weather Service for "sp[eaking] in absolute terms that were inconsistent with probabilities from the best forecast products available at the time."

To back Trump's position, the NOAA statement pointed to a wind-speed probability graphic, saying that it "demonstrated that tropical-storm-force winds from Hurricane Dorian could impact Alabama." But the graphic showed that by the morning of September 1, forecasters predicted less than a 10% chance of tropical storm-force winds reaching a small part of southeast Alabama. The rest of Alabama faced no risk of tropical storm-force winds. By definition, tropical storm-force winds are between 39 and 73mph, while hurricanes start at 74mph.

Enlarge / NOAA graphic on Hurricane Dorian.

Multiple investigations ongoing

The Commerce Department's inspector general "is investigating how that [NOAA] statement came to be issued, saying it could call into question scientific independence," the Times wrote. The House of Representatives committee on science, space, and technology is also investigating.

NOAA Research Assistant Administrator Craig McLean wrote a message Monday to all NOAA Research employees addressing what he called "a complex issue involving the President commenting on the path of the hurricane." McLean wrote that the NOAA press release backing Trump's position is "very concerning as it compromises the ability of NOAA to convey life-saving information necessary to avoid substantial and specific danger

to public health and safety.

“My understanding is that this intervention to contradict the forecaster was not based on science but on external factors including reputation and appearance, or simply put, political,” McLean wrote in the message, which was published on the NOAA website.

McLean backed the forecaster or forecasters who contradicted Trump, saying they “corrected any public misunderstanding in an expert and timely way, as they should.” McLean also wrote that the press release “violated NOAA’s policies of scientific integrity.”

McLean is not done investigating the matter. “In my role as Assistant Administrator for Research, and as I continue to administratively serve as Acting Chief Scientist, I am pursuing the potential violations of our NOAA Administrative Order on Scientific Integrity,” he wrote.

https://arstechnica.com/?p=1567459

Web scraping doesn’t violate anti-hacking law, appeals court rules

Enlarge / LinkedIn CEO Jeff Weiner.

reader comments

95 with 53 posters participating

Share this story

Scraping a public website without the approval of the website's owner isn't a violation of the Computer Fraud and Abuse Act, an appeals court ruled on Monday. The ruling comes in a legal battle that pits Microsoft-owned LinkedIn against a small data-analytics company called hiQ Labs.

HiQ scrapes data from the public profiles of LinkedIn users, then uses the data to help companies better understand their own workforces. After tolerating hiQ's scraping activities for several years, LinkedIn sent the company a cease-and-desist letter in 2017 demanding that hiQ stop harvesting data from LinkedIn profiles. Among other things, LinkedIn argued that hiQ was violating the Computer Fraud and Abuse Act, America's main anti-hacking law.

This posed an existential threat to hiQ because the LinkedIn website is hiQ's main source of data about clients' employees. So hiQ sued LinkedIn, seeking not only a declaration that its scraping activities were not hacking but also an order banning LinkedIn from interfering.

A trial court sided with hiQ in 2017. On Monday, the 9th Circuit Appeals Court agreed with the lower court, holding that the Computer Fraud and Abuse Act simply doesn't apply to information that's available to the general public.

"The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically computer hacking," a three-judge panel wrote. The court notes that members debating the law repeatedly drew analogies to physical crimes like breaking and entering. In the 9th Circuit's view, this implies that the CFAA only applies to information or computer systems that were private to start with—something website owners

typically signal with a password requirement.

The court notes that when the CFAA was first enacted in the 1980s, it only applied to certain categories of computers that had military, financial, or other sensitive data.

“None of the computers to which the CFAA initially applied were accessible to the general public,” the court writes. “Affirmative authorization of some kind was presumptively required.”

When the law was extended to more computers in 1996, a Senate report said its goal was to “increase protection for the privacy and confidentiality of computer information.” As a result, the 9th Circuit reasons “the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort.”

By contrast, hiQ is only scraping information from public LinkedIn profiles. By definition, any member of the public has authorization to access this information. LinkedIn argued that it could selectively revoke that authorization using a cease-and-desist letter. But the 9th Circuit found this unpersuasive. Ignoring a cease-and-desist letter isn’t analogous to hacking into a private computer system.

LinkedIn can’t interfere with hiQ’s scraping

Monday’s ruling goes beyond finding that hiQ hasn’t violated anti-hacking laws. The appeals court also upheld a lower court order banning LinkedIn from interfering with hiQ’s scraping activities during the course of the litigation.

HiQ argues that if LinkedIn started using technical measures to block hiQ from scraping LinkedIn user data, it would be interfering with hiQ’s contracts with its own customers, who

rely on that data (this is known in legal jargon as “tortious interference with contract”). HiQ noted that LinkedIn tacitly accepted hiQ’s scraping activities for several years—even sending representatives to hiQ conferences where hiQ openly explained that its products were built on LinkedIn data.

LinkedIn argued that it needed to restrict scraping to protect its own users’ privacy. But hiQ countered that the data didn’t belong to LinkedIn but to its users—who explicitly marked the data public. HiQ doesn’t scrape non-public LinkedIn profiles. HiQ also says that LinkedIn only objected to hiQ’s scraping around the time LinkedIn launched its own analytics tools that competed with hiQ’s offerings.

Taking all of this into account, the appeals court ruled that hiQ had a good chance of proving that it was entitled to continue scraping LinkedIn’s data during the legal battle. LinkedIn might still prevail on this point, eventually giving the company the right to blacklist hiQ’s scrapers. But the appeals court upheld the lower court’s order that LinkedIn wait until after the court case was over before doing so. Otherwise, hiQ might be out of business before it had a chance to finish the case.

This remains an unsettled area of the law. In 2013, for example, a California federal trial court held that two companies may have violated the Computer Fraud and Abuse Act when they scraped data from Craigslist in order to provide user-friendly alternatives for viewing Craigslist listings.

Like the hiQ case, this early one occurred in California, so appeals would have been heard by the 9th Circuit—which might have been sympathetic to their case. But the defendants didn’t get that far—they settled the case in 2015 and agreed to stop scraping Craigslist content. Monday’s ruling suggest that they might have actually prevailed on appeal.

https://arstechnica.com/?p=1564309