

Please **create an account** to participate in the Slashdot moderation system

Nickname:

Password:

6-1024 characters long

☐ Public Terminal

Log In

[Forgot your password?](#)

Log in With Google

Log in With Facebook

Log in With Twitter

Log in With LinkedIn

[Close](#)

Check out Slashdot on [LinkedIn](#) & [Minds!](#) | Migrate from GitHub to SourceForge quickly and easily with [this tool](#). Check out all of SourceForge's [improvements](#).





OnePlus Notifies Customers of Data Breach Impacting Users of Its Online Store

Posted by [BeauHD](#) on Friday November 22, 2019 @06:20PM from the [here-we-go-again](#) dept.


OnePlus has sent out an email [informing recent OnePlus customers of a security issue](#). "This 'Security Notification' from OnePlus informs customers that an 'unauthorized party' was able to access order information

from the company's online store," reports 9to5Google. "OnePlus says that payment information as well as account details were not accessed, but names, addresses, emails, and phone numbers 'may' have been exposed. The company says it will continue to investigate the matter, but obviously this is no small issue." From the report: *Speaking to [Droid-Life](#), OnePlus says that they took "immediate steps to stop the intruder and reinforce security," and that they are currently "working with the relevant authorities to further investigate this incident." OnePlus didn't explain what went wrong, but they are apparently working to start a bug bounty program by the end of this year.*

This isn't the first time the company's store has fallen victim to a security issue like this. In early 2018, OnePlus customers [found evidence of credit card fraud](#) stemming from the Store that triggered OnePlus to shut down credit card payments temporarily. Just a day later, OnePlus' investigation into the matter revealed that 40,000 credit card numbers had been exposed. OnePlus [has a thread on its forums](#) with more details about the breach.



DOD Joins Fight Against 5G Spectrum Proposal, Citing
Risks To GPS (arstechnica.com)

android data security 

 Posted by BeauHD on Friday November 22, 2019 @05:45PM from the pros-and-cons dept.

An anonymous reader quotes a report from Ars Technica: [The Department of Defense has weighed in against a proposal before the Federal Communications Commission to open the 1 to 2 Gigahertz frequency range -- the L band -- for use in 5G cellular networks. The reason: segments of that range of radio spectrum are already used by Global Positioning System signals and other military systems. In a letter to FCC Chairman Ajit Pai, Secretary of Defense Mark Esper \[pressed for the rejection of the proposal by Ligado Networks\]\(#\) \(formerly known as Lightspeed\), saying, "There are too many unknowns and the risks are far too great to federal operations to allow Ligado's proposed system to proceed... This could have a significant negative impact on military operations, both in peacetime and war."](#)


The FCC has already largely brushed aside similar opposition from NASA, the US Navy, and the National Oceanographic and Atmospheric Administration, among others, over another spectrum block in the 24GHz range -- which is used by weather satellites for remote monitoring of water vapor. But comments are still being collected on the Ligado plan for sharing the 1675 to 1680MHz block of the L Band. Pai has been supportive of the plan because that range is adjacent to the existing 1670 to 1675MHz block already in use for wireless services. GPS signals use several blocks of the L band, including a primary channel centered on 1575.42MHz. GPS uses L band signals because of their ability to penetrate cloud cover, rain, and vegetation. The L band is also used by the DOD for a [number of other purposes](#), including tactical air navigation, landing assistance telemetry, Identify Friend or Foe (IFF) signals, and missile range and aircraft telemetry -- though the DOD has already had to move some of these applications further up the spectrum range to make room for previous "commercial reallocation."



View Active Directory Permissions at a Glance

fcc gps military 

Posted by Slashdot

Get your free AD permissions assessment with Access Rights Manager.
Access Rights Manager (ARM) visualizes who can access a given resource at your organization. In a central view, you can see the group memberships from Active Directory  and the access rights given.

Try it FREE for 30 days!

[Slashdot Deals](#)

Sacha Baron Cohen Gave the Greatest Speech on Why Social Networks Need To Be Put On Check (zdnet.com)



Posted by msmash on Friday November 22, 2019 @05:05PM from the how-about-that dept.

For an actor who made a career by playing silly characters, actor Sacha Baron Cohen gave yesterday one of the most eloquent and convincing speeches in a long time in support of [cracking down on large social media networks to prevent the spread of lies and hate speech that these platforms allow](#). From a report: *While accepting his award, Cohen touched on the role companies like Facebook, Google, and Twitter have played in spreading lies and hate speech online, calling the sites "the greatest propaganda machine in history." Below is a short summary of his main talking points. Cohen called Facebook, YouTube and Google, Twitter and others -- the biggest propaganda machine in history. He coined the term "Silicon Six" to describe the six US billionaires that control this machine -- naming Zuckerberg at Facebook, Sundar Pichai at Google, Larry Page and Sergey Brin at Alphabet, Susan Wojcicki at YouTube, and Jack Dorsey at Twitter. The actor ripped Zuckerberg for defending holocaust deniers.*

He ripped Zuckerberg for his platform facilitating Russia's interference in US elections. He ripped Zuckerberg for facilitating the Myanmar genocide. Said if another genocide takes place, Zuckerberg needs to go to jail. Cohen ripped Facebook for allowing political ads. Said if Facebook existed in the 1930s they would have allowed Hitler to post "post 30-second ads on his 'solution' to the 'Jewish problem'." Cohen likened the Christchurch massacre video to "a snuff film broadcast by social media." He said social media sites are today's largest publishers, and should have to abide to the same standards that newspapers, radio, and TV stations abide. He agreed that social media should function based on government-mandated rules, and not by internal policies set by billionaires more focused on protecting share prices than human life. He called "for regulation and legislation to curb the greed of these high-tech robber barons."



Facebook Built a Facial Recognition App That Let Employees Identify People By Pointing a Phone at Them

media social technology



(businessinsider.com)



Posted by msmash on Friday November 22, 2019 @04:22PM from the how-about-that dept.

Facebook once built an internal app that let employees [identify people using facial recognition and their phone cameras](#), *Business Insider* reported Friday. From the report: *The app, which was developed between 2015 and 2016, utilised Facebook's vast collection of user identities to automatically recognise the person at whom the phone's camera was pointed. The app was not released publicly, and Facebook tells Business Insider that it only worked on company employees and any of their friends who opted in to the social network's facial recognition system. "As a way to learn about new technologies, our teams regularly build apps to use internally. The apps described here were only available to Facebook employees, and could only recognize employees and their friends who had face recognition enabled," said a Facebook spokesperson. The existence of the app illustrates how Facebook has been quick to experiment with technology that could have significant societal implications.*



1.2 Billion Records Found Exposed Online in a Single Server (wired.com)

facebook privacy facialrecognition



Posted by msmash on Friday November 22, 2019 @03:45PM from the security-woes dept.

Slashdot Poll

Are you a fan of the new Tesla Cybertruck?

☐ Yes

☐ No

☐ Not sure yet

JustAnotherOldGuy writes: For well over a decade, identity thieves, phishers, and other online scammers have created a black market of stolen and aggregated consumer data that they used to break into people's accounts, steal their money, or impersonate them. In October, dark web researcher Vinny Troia found one such trove sitting exposed and easily accessible on an unsecured server, [comprising 4 terabytes of personal information -- about 1.2 billion records in all](#). While the collection is impressive for its sheer volume, the data doesn't include sensitive information like passwords, credit card numbers, or Social Security numbers. It does, though, contain profiles of hundreds of millions of people that include home and cell phone numbers, associated social media profiles like Facebook, Twitter, LinkedIn, and Github, work histories seemingly scraped from LinkedIn, almost 50 million unique phone numbers, and 622 million unique email addresses. "It's bad that someone had this whole thing wide open," Troia says. "This is the first time I've seen all these social media profiles collected and merged with user profile information into a single database on this scale. From the perspective of an attacker, if the goal is to impersonate people or hijack their accounts, you have names, phone numbers, and associated account URLs. That's a lot of information in one place to get you started."

vote now

[Read the 23 comments](#) | 1142 votes

[f](#) [t](#) [in](#) [r](#) **FCC Bars Huawei, ZTE From Billions in Federal Subsidies** [\(cnet.com\)](#) [internet](#) [privacy](#) [security](#) [🔒](#)



Posted by msmash on Friday November 22, 2019 @03:10PM from the tussle-continues dept.

The US Federal Communications Commission on Friday voted to bar use of its [\\$8.5 billion a year Universal Service Fund to purchase equipment and services from Huawei](#) and ZTE. The government fund is used by multiple programs to subsidize US broadband deployment and services. From a report: *In a unanimous vote during its November open meeting, the FCC approved an order that blocks the use of USF funds to purchase equipment and services from companies that pose a national security threat. The order also establishes a process for barring more companies in the future. So far, just Huawei and ZTE are on the list. "Given the threats posed by Huawei and ZTE to America's security and our 5G future, this FCC will not sit idly by and hope for the best," said FCC Chairman Ajit Pai in a statement Friday.*

[f](#) [t](#) [in](#) [r](#) **Astronomers Detect Water Vapor Around Jupiter's Moon Europa** [\(wired.com\)](#) [business](#) [china](#) [fcc](#) [🔒](#)



Posted by msmash on Friday November 22, 2019 @02:30PM from the how-about-that dept.

In the search for life in our solar system, Mars tends to steal the spotlight. But in recent years Jupiter's fourth largest moon, Europa, has emerged as a promising extraterrestrial nursery. Planetary scientists have long suspected Europa may harbor a vast liquid water ocean beneath its thick, icy crust. If Europa's ocean also has a source of energy -- think hydrothermal vents -- and a few choice chemical elements, [there's a decent chance it could support basic lifeforms](#). From a report: *This theory makes a lot of assumptions, but on Monday it received one of its biggest boosts yet. An international team of astronomers announced they directly detected water vapor in Europa's atmosphere for the first time. As detailed in a paper published in Nature Astronomy, this method of detection is strong evidence that liquid water exists beneath the surface of Europa. "This doesn't necessarily mean the water vapor is coming from an ocean," says NASA planetary scientist Lucas Paganini. "But it does seem like this detection is connected to liquid water under the surface." A lot of what we know about Europa was gleaned from data collected by the Galileo spacecraft on its tour of Jupiter in the late '90s. One of the most remarkable findings from that mission was that something was messing with Jupiter's magnetic field. Based on this finding, planetary scientists hypothesized Europa might be home to an electrically conductive fluid, like salt water, that was causing the magnetic disturbances.*

From The Web

[Take A Look At Who Troy Aikman Is Married To Today](#)

[FinancialAdvisorHeroes](#)

[This FOX News Anchor Makes More Money A Month Than Most Make In A Year](#)

[Weight Loss Groove](#)

[Skip the Doctor and Upgrade to the World's Smartest CPAP](#)

[Easy Breathe CPAP Company](#)

[If Your Cat Is Over 5 Years Old They Are At High Risk Of...](#)

[Dr. Marty Feline Prime | Supplement](#)

Most Discussed

453 comments [Elon Musk Unveils 'Cybertruck' Electric Pickup Truck](#)

299 comments [No, That Mac Factory in Texas Is Not New](#)

[Early 2020](#) [\(venturebeat.com\)](#)

[Posted by msmash on Friday November 22, 2019 @01:50PM from the moving-forward dept.](#)

Normally, major 5G network expansion news has been exciting enough for carriers to announce first thing in the morning, but AT&T just continued its already confusing 5G story by revealing a big change in the dead of night: It's launching a [low-band 5G network across five cities in "the coming weeks,"](#) with promises to cover at least 15 cities by February 2020. From a report: *This will be the carrier's first 5G launch targeted at regular customers. The good news: Some form of AT&T 5G service will soon be available in Indianapolis, Pittsburgh, Providence, Rochester, and San Diego, followed by Birmingham, Boston, Bridgeport, Buffalo, Las Vegas, Louisville, Milwaukee, New York City, San Francisco, and San Jose early next year. Initial service maps actually cover wide swaths of each city, in some cases extending into suburbs, and the carrier suggests the low-band 5G will work at roughly two-mile distances from towers, including "on the go," residential, "suburban," and "rural" usage.*

[Microsoft Gets Export License To Sell To Huawei](#) [att usa communications](#)

[Posted by msmash on Friday November 22, 2019 @01:11PM from the how-about-that dept.](#)

[hackingbear](#) writes: *Microsoft has been granted [a license to export \[mass market\] software to Huawei](#) once again. The software giant was caught up in a long line of US-based technology companies that have been forced to comply with President Trump's executive order to crack down on Chinese tech companies. It's not immediately clear what "mass-market" refers to, but Microsoft sells Windows and Office licenses to Huawei. It's likely that Microsoft is at least able to sell Windows licenses to Huawei once again, which will help with Huawei's server solutions and its Windows-powered laptops. Microsoft is part of a number of US companies that are starting to get licenses to supply goods to Huawei once again. Huawei [has been anticipating a fight with the US](#) and prepared and [succeed in replacing American \(electronic\) technologies](#) with its own home-grown replacement for almost two decades after [Motorola foolishly rejected the chance of acquiring Huawei](#), China's most successful hi-tech company worth at least \$100 billion today, over a bargaining price of \$7.5 billion. "When this decision was made, I told them [Huawei executives], if we continued to work in this sector, we would definitely be in a race against the US in 10 years. We had to prepare", said then Huawei founder Ren Zhengfei after the merger fell through. However, software ecosystems, i.e. Windows and Android, remain Huawei's Achilles' heel.*

[How Lax Oversight Of Electronic Health Records Puts Patients At Risk](#) [business china it](#)

[Posted by msmash on Friday November 22, 2019 @12:21PM from the closer-look dept.](#)

Plans to ensure patient safety as the nation transitioned to electronic health records have [yet to come to fruition a decade later](#), according to a new report. From an investigation: *In fall 2009, several dozen of the best minds in health information technology huddled at a hotel outside Washington, D.C., to discuss potential dangers of an Obama White House plan to spend billions of tax dollars computerizing medical records. The health data geeks trusted that transitioning from paper to electronic records would cut down on medical errors, help identify new cures for disease and give patients an easy way to track their health care histories. But after two days of discussions, the group warned that few safeguards existed to protect the public from possible consequences of rolling out the new technology so quickly. Because this software tracks the medicines people take and their vital signs, even a tiny error or omission, or a doctor's inability to access the file quickly, can be a matter of life or*

- 114 comments [Ayahuasca Alters Brain Waves To Produce Waking Dream-Like State, Study Finds](#)
- 108 comments [Ride-Hailing Apps Have Allowed More Binging and Increased Demand For Bartenders](#)
- [Ask Slashdot: How Do You Teach Inventing To Kids?](#)
- [Ask Slashdot: What Happened To Holographic Data Storage?](#)
- [Ask Slashdot: What Should You Do If Someone's Trying To Steal Your Identity?](#)
- [Bring Back the Replaceable Laptop Battery'](#)
- [Are Forced Subscriptions Driving 3D Users To Open Source Tools?](#)

[This Day on Slashdot](#)

2013	A War Over Solar Power Is Raging Within the GOP	1030 comments
2011	Debt Reduction Super Committee Fails To Agree	954 comments
2006	Creationism Museum To Open Next Summer	1570 comments
2005	Ask The Mythbusters	1435 comments
2002	Another Millionaire Spammer Story	979 comments






[Sourceforge Top Downloads](#)

- [TrueType core fonts 2.2B downloads](#)
- [Notepad++ Plugin Mgr 1.5B downloads](#)
- [VLC media player 899M downloads](#)
- [eMule 686M downloads](#)
- [MinGW 631M downloads](#)

Powered By
[sf](#)

death. The experts at that September 2009 meeting, mainly members of the American Medical Informatics Association, or AMIA, agreed that safety should be a top priority as federal officials poured more than \$30 billion into subsidies to wire up medical offices and hospitals nationwide. The group envisioned creating a national databank to track reports of deaths, injuries and near misses linked to issues with the new technology. It never happened.

Instead, plans for putting patient safety first -- and for building a comprehensive injury reporting and reviewing system -- have stalled for nearly a decade, because manufacturers of electronic health records (EHRs), health care providers, federal health care policy wonks, academics and Congress have either blocked the effort or fought over how to do it properly, an ongoing investigation by Fortune and Kaiser Health News shows. Over the past 10 years, the parties have squabbled over how best to collect injury data, over who has the power to require it, over who should pay for it, and over whether to make public damning findings and the names of those responsible for safety problems. In 2015, members of Congress derailed a long-planned EHR safety center, first by challenging the government's authority to create it and later by declining to fund it. A year later, Congress stripped the Food and Drug Administration of its power to regulate the industry or even to track malfunctions and injuries.

    **Twitter Will Finally Let Users Disable SMS as Default 2FA** [health politics usa](#) 
Method ([zdnet.com](#))



Posted by msmash on Friday November 22, 2019 @11:42AM from the security-woes dept.




Twitter says users will finally be able to [disable SMS-based two-factor authentication \(2FA\) for their accounts](#), and use an alternative method only, such as a mobile one-time code (OTP) authenticator app or a hardware security key. Until this week, this was impossible. From a report: *If users wanted to use 2FA for their Twitter account, they had to register a phone number and enable the SMS-based 2FA method, even if they wished it or not. Users who wanted to use an OTP mobile authenticator app or a hardware security key, had to enable the SMS-based 2FA first, and they couldn't disable it. Even if the user chose to use a security key, the SMS-based 2FA method was still active, and exposed the account to attacks known as SIM swaps. Hackers who knew a user's password would perform a SIM swap to temporarily hijack a user's phone number, bypass SMS-based 2FA, and then take over that user's account.*

    **'The Ducks Have Won': French Court Says** [security twitter twofactorauthentication](#) 
They May Keep on Quacking ([reuters.com](#))



Posted by msmash on Friday November 22, 2019 @11:02AM from the meanwhile-in-some-other-news dept.

The ducks on a small French smallholding may carry on quacking, a French court ruled this week, [rejecting a neighbor's complaint that the birds' racket was making their life a misery](#). From a report: *The court in the town of Dax ruled that the noise from the flock of around 60 ducks and geese kept by retired farmer Dominique Douthe in the foothills of the Pyrenees, southwestern France, was within acceptable limits, broadcaster France 3 said. "The ducks have won," Douthe told Reuters after the court decision. "I'm very happy because I didn't want to slaughter my ducks." The complaint was brought by Douthe's neighbor who moved from the city around a year ago into a property about 50 meters (yards) away from the enclosure in the Soustons district where Douthe keeps her flock. The dispute is the latest in a series of court cases that have pitted the traditional way of life in rural France against modern values which, country-dwellers say, are creeping in from the city.*

    [court technology nimby](#) 

Apple CEO Tim Cook: China Really Hasn't Pressured Us. (9to5mac.com)



Posted by msmash on Friday November 22, 2019 @10:21AM from the straw-man dept.

[hackingbear](#) writes: *In a talk with ABC News, Apple CEO Tim Cook discussed Apple's investment in the United States, his relationship with President Trump, China and more. When asked if there was a line Apple would not cross if China pressured the company [to violate user's privacy and rights], Cook said [they have never been asked in China by authorities to unlock an iPhone](#), but added, referring to the U.S., "I have here. And we stood up against that, and said we can't do it," he added. "Our privacy commitment is a worldwide one." When asked why Apple still builds the iPhone in China, Cook said that he actually thinks "the iPhone is made everywhere." "If you look at the glass of the iPhone, which everybody touches all day long, that glass is made in Kentucky. If you were to take apart the iPhone you would see many of the silicone components that are made in the United States as well," he added. "The iPhone is the product of a global supply chain." John Gruber of DaringFireball adds: If China hasn't pressured Apple, why was the [Taiwanese flag emoji removed from iOS devices in Hong Kong](#)? It's far from the biggest issue surrounding China. I get that. It's just a flag emoji, and we're talking about a regime that has put over a million people into concentration camps. But it is bullshit. Under the one-country-two-systems arrangement China itself agreed to regarding Hong Kong, there is nothing illegal about the Taiwanese flag. It's flat-out wrong that Apple removed the Taiwanese flag emoji in Hong Kong. But if they did so at the behest of China at least we'd have a reason why. If China hasn't pressured Apple on this point, small though it may be, why in the world did Apple remove the flag? [It reeks of cowardice](#). **Further reading:** [Apple Has No Backbone](#).*



One-Third of Tropical African Plant Species at Risk of Extinction (sciencemag.org)

[apple](#) [china](#) [privacy](#)



Posted by msmash on Friday November 22, 2019 @09:41AM from the closer-look dept.

A third of plant species in tropical Africa are threatened with extinction, a new study suggests. Plants are crucial to many ecosystems and life in general, providing food and oxygen, as well as being the source of myriad materials and medicines. However, [human activities including logging, mining and agriculture pose a major threat](#). From a report: *While the extinction risk of animals around the world has been well studied, the risk facing many plants remains unclear: 86% of mammal species have been assessed by the International Union for Conservation of Nature (IUCN) for its Red List, compared with only 8% of plant species. Now experts say they have come up with a rapid approach to give a preliminary classification. "Our approach can help to prioritise either species or regions on which proper IUCN Red Listing should focus," said Dr Gilles Dauby of the French National Research Institute for Sustainable Development and a co-author of the research.*

He said the list was recognised as an authoritative source, and was crucial to planning projects that could affect the environment. The new study is the latest to throw the plight of plants into the spotlight. Earlier this year, scientists completed the most thorough analysis to date of plant extinctions, finding that 571 species had been wiped out since the start of the industrial revolution -- a figure they say is likely to be an underestimate. Writing in the [journal Science Advances](#), Dauby and colleagues report how they focused on two IUCN Red List criteria -- one relating to population size reduction and the other to habitat decline -- to develop a computer algorithm to automatically classify the conservation status of plants.



Oxford Dictionaries Declares 'Climate Emergency' the Word of 2019 (theguardian.com)

[science](#) [earth](#) [nature](#)





Posted by msmash on Friday November 22, 2019 @09:01AM from the for-the-record dept.

Oxford Dictionaries has [declared "climate emergency" the word of the year for 2019](#), following a hundred-fold increase in usage that it says demonstrated a "greater immediacy" in the way we talk about the climate. From a report: *Defined as "a situation in which urgent action is required to reduce or halt climate change and avoid potentially irreversible environmental damage resulting from it," Oxford said the words soared from "relative obscurity" to "one of the most prominent -- and prominently debated -- terms of 2019." According to the dictionary's data, usage of "climate emergency" soared 10,796%. Oxford said the choice was reflective, not just of the rise in climate awareness, but the focus specifically on the language we use to discuss it. The rise of "climate emergency" reflected a conscious push towards language of immediacy and urgency, the dictionary said. In 2019, "climate" became the most common word associated with "emergency," three times more than "health emergency" in second.*



[science](#) [climatechange](#) [earth](#)



[« Newer](#) [Older »](#)

Sponsored Content

Sponsored Links by Taboola

Brad Pitt's Daughter Is Probably The Prettiest Girl Alive

Best Of Senior

15 States Where Americans Don't Want To Live Anymore

MoneyWise.com

New Fix Proven To Fight Dog Gum Disease - Fast

Petlab Co.

The New Budget SmartWatch, Everyone In United States Is Talking About

eWatch

Seniors Born Before 1969 With No Life Insurance Should Do This Before It's Too Late

National Family Life Insurance Quotes

Looking for a plumber in Seattle? See ads

Plumbing Services | Search Ads

[Slashdot](#)

[Today](#)

[Thursday](#)

[Wednesday](#)

[Tuesday](#)

[Monday](#)

[Sunday](#)

[Saturday](#)

[Friday](#)

[Submit Story](#)

"Well I don't see why I have to make one man miserable when I can make so many men happy." -- Ellyn Mustard, about marriage

[FAQ](#)

[Story Archive](#)

[Hall of Fame](#)

[Advertising](#)

[Terms](#)

[Privacy Statement](#)

[Opt-out Choices](#)

[About](#)

[Feedback](#)

[Mobile View](#)

[Blog](#)

Trademarks property of their respective owners. Comments owned by the poster. Copyright © 2019 SlashdotMedia. All Rights Reserved.

[Close](#)

[Slashdot](#)

Working...