Nikki Haley lost her password, so she sent confidential info over unclassified system



Enlarge / Ambassador Nikki Haley listens at the United Nations.

reader comments

241 with 105 posters participating

Share this story

Former US Ambassador to the United Nations Nikki Haley sent confidential material over a network reserved only for unclassified material because she forgot her password for classified communications, The Daily Beast reported.

The event happened on July 4 and July 5, 2017, after North Korea had tested an intercontinental ballistic missile capable of hitting Alaska. As she and her staff scrambled to draft a statement responding to the test, Haley reportedly used her BlackBerry 10 to trade comments over the OpenNet, a State Department network for communicating sensitive, but not classified, information.

“Can’t find my password,” she wrote on July 5. Other messages instructed staff to make changes to the preliminary statement versions they had drafted.

The revelation was disclosed in emails watchdog organization American Oversight obtained under the Freedom of Information Act. The incident comes after Haley’s boss, President Donald Trump, castigated his campaign rival Hillary Clinton for sending classified material over her private email server. His chant to “lock her up” became a constant refrain for him and his supporters.

It’s arguable that the OpenNet is more secure than a private email address. Still, there’s a reason the State Department system isn’t suitable for transmitting classified material. Last year, Politico reported that the State Department’s unclassified email system suffered a breach that exposed the personal information of a small number of employees.

Watchdog groups have repeatedly criticized the State Department for what they say is insufficient network security. By the time the 2018 breach came to light, a bipartisan group of senators had already asked Secretary of State Mike Pompeo what the department was doing to improve things.

Given the growing determination and skill of hackers sponsored by the governments of North Korea, Iran, Russia, and China, unclassified systems are increasingly vulnerable to espionage. Staff members for Haley, who resigned her ambassador post in October of last year, didn’t provide a comment to Politico.

Post updated on 11/20/2019, 6:49 PM to change “sensitive” to “confidential” per original article.

https://arstechnica.com/?p=1604835

As DirecTV tanks, AT&T says it will “re-bundle” TV with HBO Max



Enlarge / AT&T executive John Stankey at a presentation for investors at Warner Bros. Studios on October 29, 2019, in Burbank, California.

reader comments

73 with 62 posters participating

Share this story

AT&T’s traditional TV business is tanking, with the company having lost nearly 5 million satellite and wireline TV customers since the end of 2016.

But AT&T President John Stankey sees a path forward in recreating the traditional cable-TV bundle on the Internet. AT&T’s HBO Max is slated to launch in May 2020 for $14.99 a month, and AT&T has set an ambitious goal of 50 million US subscribers within five years.

A subscriber number like that would make HBO Max far bigger than AT&T’s DirecTV satellite division and its U-verse wireline TV service. But ultimately, the service customers get could end up looking pretty similar to DirecTV, U-verse, or cable TV.

“Stankey said the vision for HBO Max is to create a bundle of content that includes movies and shows not owned by WarnerMedia in addition to those it creates and licenses on its own,” Vox wrote yesterday in a report titled “HBO Max wants to be the next cable bundle instead of the next Netflix.” The report summarizes an interview Stankey gave at Recode’s Code Media conference.

HBO Max will “at some point in time” be “a platform that we allow others to bring content into,” Stankey said. “I don’t think, from my point of view, we’re ever going to have a lock or a monopoly on creativity.”

“Re-aggregate and re-bundle”

Stankey, a 34-year AT&T employee who is president and chief operating officer, is second-in-command to AT&T CEO Randall Stephenson and may be in line to become CEO when Stephenson retires. He is also CEO of WarnerMedia, the AT&T division that includes HBO.

Stankey noted that the proliferation of online video services has caused the traditional cable bundle to “fragment” into multiple platforms. Customers are frustrated about “the fragmentation of the bundle,” but AT&T can bring the bundle back together, Stankey said.

“We’re basically unbundling to re-bundle,” Stankey said. “At some point, there will be platforms that re-aggregate and re-bundle, and we’d like the [HBO Max] platform ultimately to be a place where re-aggregation occurs. And that doesn’t just mean our content.”

You can see the whole Stankey interview in the video below. The bundling discussion starts at 29:10:

[embedded content]
AT&T’s John Stankey and Recode Senior Media Correspondent Peter Kafka onstage at Code Media 2019 in Los Angeles.

With AT&T, expect price increases

If AT&T fully recreated the cable bundle and still charged $14.99 a month for all of it, that’d be a good deal. But that isn’t likely, as AT&T has already developed a history of raising online streaming prices to amounts far greater than the introductory prices.

DirecTV Now, AT&T’s online alternative to DirecTV satellite service, was initially pitched in 2016 as a $35-per-month plan with more than 100 channels. But AT&T has raised prices multiple times and lowered the number of channels by removing ones that aren’t part of the AT&T-owned Time Warner Inc.

The service, since renamed “AT&T TV Now,” today costs $65 a month for 45 channels including HBO. Packages with more than 100 channels cost at least $124 a month, while the “Ultimate” package costs $135 a month for 125 channels.

At $14.99 a month, HBO Max’s price would be similar to

Netflix's standard and premium offerings that cost $12.99 and $15.99, respectively. HBO Max's price would also be identical to the current price of HBO Now, even though HBO Max would have all the HBO content plus other stuff. But as we noted with the DirecTV Now example, it wouldn't be surprising to see AT&T raise HBO Max prices significantly in the years after it launches.

AT&T scoffs at net neutrality concerns

AT&T becoming a bigger player in online video would raise net neutrality concerns, because AT&T could use its control over home and mobile broadband networks to steer customers away from rival online services and toward AT&T's.

In yesterday's Recode interview, Stankey claimed that it would be ridiculous for anyone to worry at all about AT&T or other ISPs acting in anti-competitive ways with online streaming.

"You'd be hard-pressed to point to an instance of anybody's behavior that would suggest that there is any kind of discrimination, favoritism, or anything else going on in how people get to content on the Internet over a broadband connection," Stankey said. "It's a problem that's non-existent. There's absolutely nothing that's occurring."

Stankey would prefer that consumers direct their ire elsewhere. "I'd be far more concerned over the scale of what's occurring in terms of distribution platforms on mobile OSes, in terms and conditions associated with new product development on that and what that does to squash innovation, than anything to do with how traffic over the Internet is being treated today," he said.

But Stankey is wrong that AT&T hasn't shown "favoritism" in its treatment of video services. The Federal Communications

Commission in January 2017 accused AT&T and Verizon of violating net neutrality rules by allowing their own video services (including AT&T's DirecTV) to stream on their mobile networks without counting against customers' data caps, while charging other video providers for the same data cap exemptions.

FCC Chairman Ajit Pai rescinded that finding shortly after taking over, but that doesn't change the fact that AT&T gave its own video content favorable treatment under the data caps imposed on its mobile service.

Currently, AT&T imposes data caps ranging from 150GB to 1TB on most of its home broadband plans, which can make it hard for TV watchers to get rid of cable or satellite and use online streaming exclusively. But AT&T gives customers an upgrade to unlimited data if they pay an extra $30 a month or subscribe to DirecTV or U-verse TV. That means customers who prefer online streaming to AT&T's own TV services could have to pay $30 a month extra to get enough data or pay $10 for each additional 50GB.

Under these schemes, AT&T hasn't intentionally harmed the streaming performance of Netflix and other third-party services. But AT&T has made it more expensive for customers on AT&T broadband connections to make extensive use of those third-party services. The company has also used the unlimited-data perk to push customers toward AT&T's own TV services.

The old net neutrality rules didn't include a ban on data caps or zero-rating schemes that exempt content from data caps, but the FCC evaluated individual implementations to determine whether they were anti-competitive or anti-consumer. Since the Trump administration's repeal, the FCC hasn't enforced any net neutrality rules or scrutinized data-cap practices. But Washington state is enforcing a net neutrality law, and states including California intend to do so in the future after all appeals are exhausted in a lawsuit over the FCC's repeal of

net neutrality rules.

Stankey says that AT&T won't abuse its control over broadband networks regardless of whether net neutrality rules are enforced in the future. "There was nothing [in terms of ISPs discriminating]. It's not happened," he said yesterday. "We all want a good broadband connection that people can use to get wherever they want to get."

https://arstechnica.com/?p=1604445

Comcast trying to drive local sports network out of business, lawsuit says



Enlarge / Nikola Jokic of the Denver Nuggets makes the game-winning shot against the Philadelphia 76ers on November 8, 2019 at the Pepsi Center in Denver, Colorado.
Getty Images | Bart Young

reader comments

45 with 33 posters participating

Share this story

A lawsuit filed against Comcast today accuses the cable company of using its market power to try to drive a regional sports network out of business.

The lawsuit was filed in US District Court in Colorado by Altitude Sports, a network that broadcasts games played by the Denver Nuggets, Colorado Avalanche, and other local professional and college teams. Altitude has been blacked out on Comcast since August 31, as the companies haven't agreed on what price Comcast should pay to carry the network.

Filing a lawsuit is at least partly a negotiating tactic in cases like this one, but Altitude claims that this is more than a simple price dispute. Comcast is offering less than Altitude's actual costs because it wants to drive Altitude out of business and then acquire the TV rights to the Denver sports teams itself, Altitude alleges.

"This complaint alleges textbook anticompetitive conduct," Altitude lawyer William Isaacson said in an announcement of the suit. "This lawsuit aims to stop Comcast from abusing its monopoly power to impose terms on Altitude to drive it out of business and prey on Denver-region families."

Comcast would be able to "quickly and easily take over regional sports production" in the Denver area if it forces Altitude out of business, the lawsuit said.

Comcast dominates Denver TV market

Comcast owns the regional sports networks in major cities such as New York, Boston, Chicago, Philadelphia, and Washington, DC. But Altitude is owned by Kroenke Sports & Entertainment, which also owns the Nuggets and Avalanche, so Comcast has to purchase access to the channel in order to broadcast the top sports teams in Denver.

Comcast has a 57-percent share of the pay-TV market in the Denver area, compared to DirecTV's 25 percent, the lawsuit said. Comcast's dominance of the market "has increased since its first Altitude agreement over 15 years ago, as part of an unprecedented wave of [pay-TV] consolidation, expansion, and vertical integration," the lawsuit said. Altitude says this allows Comcast to exercise monopsony power, in which a buyer becomes so large that it effectively controls the market.

In the recent negotiations, Altitude offered a five-year contract renewal with terms similar to the previous deal, but Comcast demanded "dramatic cuts in rates to be paid to Altitude," Altitude's lawsuit said. Comcast also proposed moving the Altitude channel from a cable package that reaches at least 70 percent of Comcast's local subscribers to one that only 15 percent of Comcast customers subscribe to, which would lower the amount Altitude can charge for TV advertisements, the lawsuit said.

Comcast knows these proposals "are economically unsustainable for Altitude or any RSN [regional sports network]," Altitude said. The rates offered by Comcast "were entirely unreasonable and unworkable for Altitude given the costs it pays to rights holders and its production costs," the lawsuit said.

Comcast also rejected Altitude's offer of a one-year extension under the previous rates and terms, which would have given "the parties more time to negotiate a long-term solution and avoid a situation in which Altitude was blacked out by

Comcast," the lawsuit said.

Here's one of the key parts of the complaint, in which Altitude details its allegation that Comcast's long-term plan is to buy the broadcasting rights to Denver sports teams:

> *By negotiating fees and carriage that undermine an independent RSN and require it to charge below its costs, Comcast knows that it can cause any independent RSN to go out of business. Comcast may then reacquire the content by either purchasing the RSN's television rights themselves or by ensuring that the RSN becomes part of some other consolidated ownership. Once Comcast reacquires the content, the subscribers return, mitigating any longterm losses. For these reasons, Comcast is incentivized to suffer a short-term temporary loss of subscribers to achieve enormous long-term gains.*
>
> *Comcast is now using its monopsony power in the wholesale purchase of sports programming in the Denver DMA (designated market area) to drive Altitude out as a competitor in this exact manner.*
>
> *After Comcast puts Altitude out of business, Comcast will attempt either to buy Altitude or set up its own RSN to replace Altitude. This means that Comcast is not only violating the antitrust laws' prohibition on acquiring or maintaining monopoly (monopsony) power as a buyer in the Programming Market (the market where Altitude sells its productions); Comcast is also illegally attempting to monopolize the Production Market (the market in which Altitude and other RSNs compete to create programming) by replacing Altitude with Comcast's own captive RSN. Comcast's attempt to monopolize the Production Market is a separate and independent violation of the antitrust laws.*

Comcast has taken a far different approach with RSNs it owns itself, Altitude said. "Comcast has not made demands of or

imposed drastic rate cuts or carriage reductions on its own affiliated RSNs throughout the country," Altitude said. For the Comcast-owned networks, Comcast continues to "sign new contracts for rates, equal to or higher than what it previously paid to Altitude," the lawsuit said.

Altitude's lawsuit asks the court for a declaratory judgment that Comcast violated antitrust laws and "tortiously interfered" with Altitude's business relationships with sports teams and advertisers. Altitude also asked for compensatory and punitive damages and an order that Comcast "distribute Altitude's programming on reasonable, non-discriminatory terms."

Comcast charges regional sports fee

Altitude was also blacked out on DirecTV, but the blackout ended in early November when the companies agreed on a price and distribution terms. Both Comcast and DirecTV charge a monthly "Regional Sports Network" fee to cover the cost of distributing networks like Altitude. Colorado Attorney General Phil Weiser is investigating the companies' decision to keep charging the fee during the blackout.

While DirecTV owner AT&T made it difficult for customers to get refunds on that fee during the blackout, Comcast automatically issued partial bill credits to account for the blacked-out channel. Comcast justified its decision to charge the remainder of the fee by noting that it also carries AT&T SportsNet Rocky Mountain channel, which broadcasts Colorado Rockies baseball games, and the Pac-12 network that broadcasts college sports.

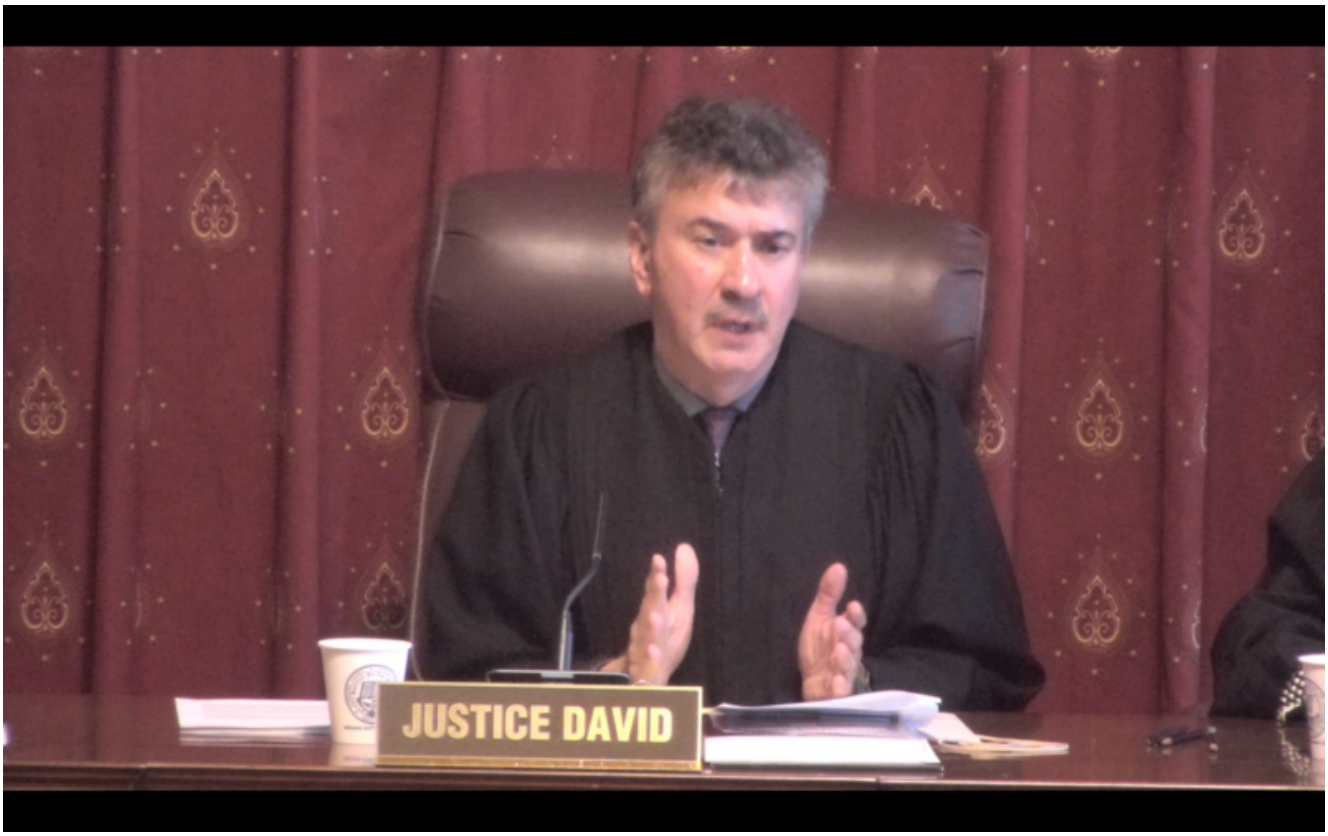
Altitude's lawsuit criticizes the Regional Sports Network fee, saying that it amounts to a "monopoly rent" charged to consumers. "The fees Comcast pays for regional sports programming in the Denver DMA dropped dramatically, but Comcast offered only a token bill reduction (as a public

relations move after consumer outcry),” Altitude said.

We contacted Comcast about Altitude’s lawsuit and will update this article if we get a response.

https://arstechnica.com/?p=1603643

Cops put GPS tracker on man’s car, charge him with theft for removing it



Enlarge / Indiana Supreme Court Justice Steven David
Indiana Supreme Court

reader comments

287 with 175 posters participating, including story author

Share this story

Back in 2012, the US Supreme Court ruled that it’s illegal for the police to attach a GPS tracking device to someone’s car without a warrant. But what if you find a GPS tracking device on your car? Can you remove it?

A little more than a year ago, the state of Indiana charged a suspected drug dealer with theft for removing a government-owned GPS tracking device from his SUV. This month, the state’s Supreme Court began considering the case, and some justices seemed skeptical of the government’s argument.

“I’m really struggling with how is that theft,” said Justice Steven David during recent oral arguments.

One time in Warrick County

The case began in July 2018, when the Warrick County Sheriff’s Office got a warrant to attach a GPS tracking device to Derek Heuring’s car. Information from a confidential informant had led them to believe that Heuring was using the vehicle to sell meth.

The GPS device transmitted data for a little more than a week. Then it stopped. Officers suspected Heuring had discovered and removed it.

After waiting another 10 days to see if it would start working again, detectives applied for a warrant to search Heuring’s home and a nearby property belonging to Heuring’s parents. US law requires law enforcement to show probable cause that a crime had been committed before engaging in a search. In this case, police said they suspected that Heuring had committed the crime of theft by taking the GPS device.

Police did find the tracking device. They also found methamphatamine and drug paraphernalia—evidence that police say show that Heuring had been dealing drugs.

So Heuring was charged both with drug dealing and with theft of the GPS device.

Is it theft to remove a GPS tracking device?

At trial, Heuring's legal team argued that the search had been illegal because the police didn't have probable cause to believe their client had committed theft. The defense pointed out that the device could have fallen off the car by accident or simply malfunctioned.

Even if Heuring did take the device off the vehicle, he couldn't have known for sure that it belonged to the government. It wasn't exactly labeled as the property of the Warrick County Sheriff's Office. Most important, it's not clear that taking an unwanted device off your car is theft—even if you know who it belongs to.

With the case now at the state Supreme Court, the stakes are high. If Heuring can show that the police lacked probable cause to search his house, he could get all of the evidence gathered in the search thrown out—not only evidence of GPS device theft, but evidence of drug dealing, too.

An appellate court ruled against Heuring in July, leading to the case reaching the Indiana Supreme Court earlier this month. Initially, multiple justices seemed skeptical of the idea that taking a tracking device off your own car amounted to theft.

"If somebody wants to find me to do harm to me and it's not the police and they put a tracking device on my car and I find a tracking device and I dispose of it after stomping on it 25 times, I would hope they would not be able to go to a local prosecutor and somehow I'm getting charges filed against me for destroying someone else's property," Justice David said.

A lawyer for the government acknowledged that it wouldn’t be theft to remove a tracking device put there by a private party. But he argued that things are different when the government has a warrant to use a tracking device. The device had a legal basis for being on the car, the lawyer argued. By removing it and preventing tracking, Heuring was depriving the government of the use of its property.

The Memorandum Decision for *Heuring v. Indiana* from the Indiana appeals court is available as a PDF through the state government’s website. The state Supreme Court is still currently considering the case after those oral arguments on November 7.

https://arstechnica.com/?p=1603367

Think of the children: FBI sought Interpol statement against end-to-end crypto



Enlarge / The Interpol HQ in France.

reader comments

110 with 88 posters participating

Share this story

Justice Department officials have long pushed for some sort of backdoor to permit warranted surveillance and searches of encrypted communications. Recently, that push has been taken international with Attorney General William Barr and his counterparts from the United Kingdom and Australia making an open plea to Facebook to delay plans to use end-to-end encryption across all the company's messaging tools.

Now, the Department of Justice and Federal Bureau of Investigations are attempting to get an even larger international consensus on banning end-to-end encryption by

way of a draft resolution authored by officials at the FBI for the International Criminal Police Organization's 37th Meeting of the INTERPOL Specialists Group on Crimes against Children. The event took place from November 12 to November 15 at the INTERPOL headquarters in Lyon, France.

A draft of the resolution viewed by Ars Technica stated that INTERPOL would "strongly urge providers of technology services to allow for lawful access to encrypted data enabled or facilitated by their systems" in the interest of fighting child sexual exploitation. Currently, it is not clear whether Interpol will issue a statement.

The draft resolution went on to lay responsibility for child exploitation upon the tech industry:

> *The current path towards default end-to-end encryption, with no provision for lawful access, does not allow for the protection of the world's children from sexual exploitation. Technology providers must act and design their services in a way that protects user privacy, on the one hand, while providing user safety, on the other hand. Failure to allow for Lawful Access on their platforms and products, provides a safe haven to offenders utilizing these to sexually exploit children, and inhibits our global law enforcement efforts to protect children.*

Attendees of the conference told Ars that the resolution's statement was due to be published this week. But in an email to the New York Times' Nicole Perlroth, an INTERPOL spokesperson denied that the resolution was considered:

> *Interpol telling me this Reuter's story is inaccurate:*
>
> *Dear Ms Perlroth,*
>
> *As per our statement there are, and were, no plans at this time for the INTERPOL General Secretariat to issue a*

> *statement in relation to encryption.*
>
> *Regards,*
> *Press Office**https://t.co/EItFe0D3Je***
>
> *— Nicole Perlroth (@nicoleperlroth)* ***November 18, 2019***

Ars requested comment from an FBI official and has not yet received a response.

Easy button

In a statement that flies in the face of the consensus of cryptographers and other technical experts, the draft resolution asserted that "technologists agree" that designing systems to "[allow] for lawful access to data, while maintaining customer privacy…can be implemented in a way that would enhance privacy while maintaining strong cyber security." In order to "honor and enforce" standards for prohibiting the distribution of "child sexual abuse material," the draft resolution states, "providers should fully comply with court orders authorizing law enforcement agencies access to data related to criminal investigations involving the sexual exploitation of children."

Facebook and other companies currently comply with warranted requests for data under the terms of the CLOUD Act—a law passed in 2018 that requires technology companies to provide data requested by warrant or subpoena to law enforcement, regardless of where in the world it is stored. But the officials behind this draft resolution claim such compliance cannot be achieved while allowing end-to-end encryption of communications.

As Barr and his compatriots noted in their October letter to Facebook, Facebook's ability to run analytics on and moderate content within users' communications amounted to 90 percent of the reports of child pornography to the National Center for

Missing and Exploited Children in 2018. By providing end-to-end encryption, officials contend, Facebook would essentially allow future child pornography distribution to “go dark” and prevent law enforcement from gathering evidence against suspects.

Today, there’s little evidence that encryption has been a major impediment to interception of communications by law enforcement to date. According to statistics from the Administrative Office of the US Courts, out of a total of 2,937 wiretaps in 2018, only 146 were encrypted—and of those, only 58 could not be decrypted.

Facebook has already deployed end-to-end encryption in products such as WhatsApp and Facebook Messenger (though Messenger does not provide end-to-end encryption by default). In response to Barr’s letter, Facebook officials responded:

> *End-to-end encryption already protects the messages of over a billion people every day. It is increasingly used across the communications industry and in many other important sectors of the economy. We strongly oppose government attempts to build backdoors because they would undermine the privacy and security of people everywhere.*

As Ars has repeatedly reported, many experts in the field of cryptography and security agree with Facebook’s assessment. The security community has largely opposed most of the pushes for encryption backdoors on the grounds that any secret “golden key” to decrypt encrypted messages would be technically infeasible—and potentially exploitable by malicious third parties.

https://arstechnica.com/?p=1603497

Google search results have more human help than you think, report finds



Enlarge / Mountain View, Calif.—May 21, 2018: Exterior view of a Googleplex building, the corporate headquarters of Google and parent company Alphabet.

reader comments

39 with 37 posters participating

Share this story

Google, and its parent company Alphabet, has its metaphorical fingers in a hundred different lucrative pies. To untold

millions of users, though, “to Google” something has become a synonym for “search,” the company’s original business—a business that is now under investigation as more details about its inner workings come to light.

A coalition of attorneys general investigating Google’s practices is expanding its probe to include the company’s search business, CNBC reports while citing people familiar with the matter.

Attorneys general for almost every state teamed up in September to launch a joint antitrust probe into Google. The investigation is being led by Texas Attorney General Ken Paxton, who said last month that the probe would first focus on the company’s advertising business, which continues to dominate the online advertising sector.

Paxton said at the time, however, that he’d willingly take the investigation in new directions if circumstances called for it, telling the Washington Post, “If we end up learning things that lead us in other directions, we’ll certainly bring those back to the states and talk about whether we expand into other areas.”

Why search?

Google’s decades-long dominance in the search market may not be quite as organic as the company has alluded, according to The Wall Street Journal, which published a lengthy report today delving into the way Google’s black-box search process actually works.

Google’s increasingly hands-on approach to search results, which has taken a sharp upturn since 2016, “marks a shift from its founding philosophy of ‘organizing the world’s information’ to one that is far more active in deciding how that information should appear,” the WSJ writes.

Some of that manipulation comes from very human hands, sources told the paper in more than 100 interviews. Employees and contractors have "evaluated" search results for effectiveness and quality, among other factors, and promoted certain results to the top of the virtual heap as a result.

One former contractor the WSJ spoke with described down-voting any search results that read like a "how-to manual" for queries relating to suicide until the National Suicide Prevention Lifeline came up as the top result. According to the contractor, Google soon after put out a message to the contracting firm that the Lifeline should be marked as the top result for all searches relating to suicide so that the company algorithms would adjust to consider it the top result.

Or in another instance, sources told the WSJ, employees made a conscious choice for how to handle anti-vax messaging:

> *One of the first hot-button issues surfaced in 2015, according to people familiar with the matter, when some employees complained that a search for "how do vaccines cause autism" delivered misinformation through sites that oppose vaccinations.*
>
> *At least one employee defended the result, writing that Google should "let the algorithms decide" what shows up, according to one person familiar with the matter. Instead, the people said, Google made a change so that the first result is a site called howdovaccinescauseautism.com—which states on its home page in large black letters, "They f—ing don't." (The phrase has become a meme within Google.)*

The algorithms governing Google's auto-complete and suggestion functions are also heavily subject to review, the sources said. Google says publicly it doesn't allow for predictions related to "harassment, bullying, threats, inappropriate sexualization, or predictions that expose private or sensitive information," and that policy's not new. The engineer who

created the auto-complete function in 2004 gave an example using Britney Spears, who at the time was making more headlines for her marriages than for her music.

The engineer “didn’t want a piece of human anatomy or the description of a sex act to appear when someone started typing the singer’s name,” as the paper describes it. The unfiltered search results were “kind of horrible,” he added.

The company has since maintained an internal blacklist of terms that are not allowed to appear in autocomplete, organic search, or Google News, the sources told the WSJ, even though company leadership has said publicly, including to Congress, that the company does not use blacklists or whitelists to influence its results.

The modern blacklist reportedly includes not only spam sites, which get de-indexed from search, but also the type of misinformation sites that are endemic to Facebook (or, for that matter, Google’s own YouTube).

Why antitrust?

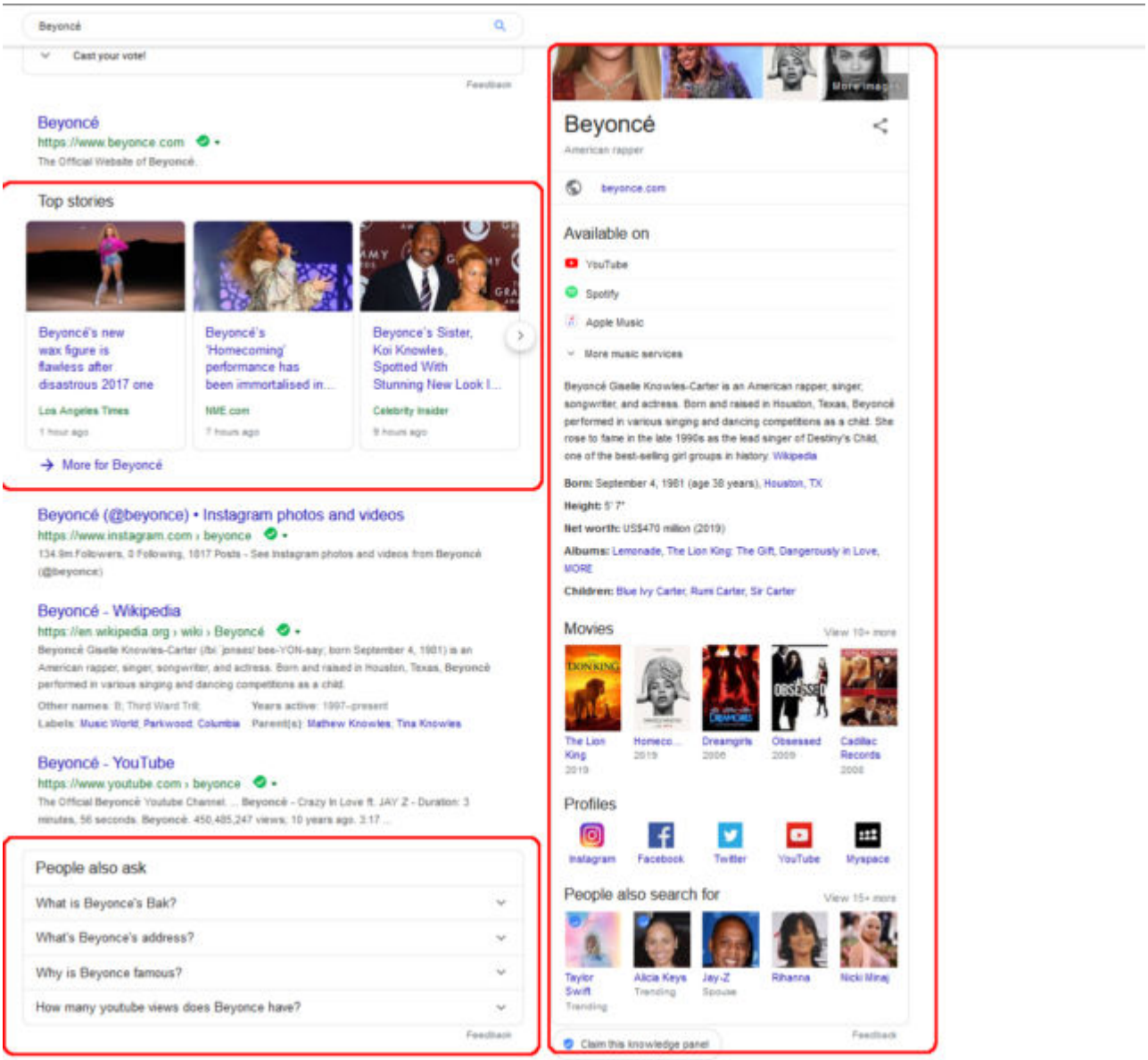
Google relying on human intervention, and endless tweaks to its algorithms as the WSJ describes, isn’t an antitrust violation. When it uses its trove of data from one operation to make choices that may harm competitors to its other operations, though, that can draw attention.

All that human intervention and algorithmic tweaking also affects advertising and business results, according to the WSJ. Those tweaks “favor big businesses over smaller ones,” the paper writes, “contrary to [Google’s] public position that it never takes that type of action.”

The largest advertisers, including eBay, have received “direct advice” on how to improve their search results after seeing traffic from organic search drop, sources told the paper.

Smaller businesses, however, have not been so lucky, being left instead to try to figure out the systems either bringing them traffic or denying them traffic on their own.

Links to Google's own features and properties also take up an increasingly large percentage of the search results page, the WSJ notes. For example, if you search for one of today's chart-toppers, such as Beyoncé, you're greeted with three large Google modules that take up more than half the screen real estate:



Enlarge / Most of the results on the page are Google modules (highlighted in red).

More than half of Google searches are now reportedly "no-click" searches, where individuals look only at the page of

results and use the snippets on it rather than clicking through to any of the sources from which Google is drawing that information. That kind of use of data, among others, could be considered harmful to competition, since the company is using data collected from competitors to keep users from going to those competitors.

Google, for its part, disputed the WSJ's findings throughout, telling the paper, "We do today what we have done all along, provide relevant results from the most reliable sources available."

https://arstechnica.com/?p=1602499

Supreme Court agrees to review disastrous ruling on API copyrights



Enlarge / Signage stands at the Oracle Corp. headquarters campus in Redwood City, California, on March 14, 2016.

reader comments

156 with 83 posters participating

Share this story

Oracle v. Google

View more stories

The Supreme Court has agreed to review one of the decade's most significant software copyright decisions: last year's ruling by an appeals court that Google infringed Oracle's copyrights when Google created an independent implementation of the Java programming language.

The 2018 ruling by the Federal Circuit appeals court "will upend the longstanding expectation of software developers that

they are free to use existing software interfaces to build new computer programs," Google wrote in its January petition to the Supreme Court.

The stakes are high both for Google and for the larger software industry. Until recently, it was widely assumed that copyright law didn't control the use of application programming interfaces (APIs)—standard function calls that allow third parties to build software compatible with an established platform like Java.

But the legal foundation of this assumption was always a bit shaky. And in 2014, the Federal Circuit Appeals Court blew it up with a ruling holding that software APIs actually can be copyrighted. A few years later, the same court held that Google's use of the Java APIs was not protected by copyright's fair use doctrine.

"The Federal Circuit's decision threatens the continued vitality of software innovation," copyright scholar James Grimmelmann told me earlier this year. He pointed out that allowing copyright protection for APIs could empower a new generation of copyright trolls that acquire the rights to old software and then sue people building newer software on top of what they thought were open standards. It could also force companies to make software that's deliberately incompatible with its rivals' products, merely to avoid getting hit with a lawsuit.

Why the case matters

The Supreme Court agrees to review only a small fraction of lower court decisions. As it often does for cases involving important policy questions, the high court asked the Trump administration to weigh in on whether the case merited Supreme Court attention. The government said no, arguing that the Federal Circuit Appeals Court had reached the right result when it held that software could be copyrighted.

But others disagreed. A number of legal scholars, public interest groups, and software companies weighed in on the case, with many arguing that the Federal Circuit's ruling would be detrimental to the software industry. Microsoft, for example, argued that the ruling "threatens the viability of the interconnected software ecosystem."

A group of legal scholars pointed out that different appeals courts have reached conflicting opinions about the legal status of APIs. This situation, known as a "circuit split," creates uncertainty about how the law will be applied in the future. The legal scholars urged the high court to take the case so it could establish a uniform legal standard nationwide.

The Supreme Court seems to have found these arguments persuasive.

The Federal Circuit Appeals Court that produced the *Google v. Oracle* ruling has become something of a whipping boy for the Supreme Court in recent years. The court has exclusive jurisdiction over patent cases nationwide, and it has used that power to make the law significantly more patent-friendly. Over the last 13 years, the Supreme Court has tried to inject some common sense back into patent law by repeatedly overturning patent-friendly decisions by the Federal Circuit.

Oracle's fight with Google focuses on copyright law, not patents. But because the case initially included some patent cases, the Federal Circuit wound up in charge of the entire case. And the nation's most pro-patent appeals court turns out to favor expansive interpretations of copyright law, too.

The Supreme Court hasn't yet announced when it will hear Google's challenge to Oracle's victory, but it's likely to occur sometime in the new year, with a ruling before the current court session wraps up at the end of June. We'll cover the case every step of the way.

https://arstechnica.com/?p=1602703

“Dirty trickster” Roger Stone convicted on all counts in Mueller indictment



Enlarge / WASHINGTON, DC – NOVEMBER 15: Former adviser to US President Donald Trump, Roger Stone departs the E. Barrett Prettyman United States Courthouse after being found guilty of obstructing a congressional investigation into Russia’s interference in the 2016 election on November 15, 2019 in Washington, DC. Stone faced seven felony charges and was found guilty on all counts.
Win McNamee / Getty Images

reader comments

269 with 104 posters participating

Share this story

Ten months after his arrest by a swarm of FBI agents, former Trump adviser and self-proclaimed “dirty trickster” Roger Stone was found guilty of all seven felony counts against him, including obstruction of Congress, five counts of false testimony to Congress, and witness tampering. The conviction is the eighth guilty sentence or plea resulting from grand jury indictments spawned by the investigations into Russian election interference by Special Counsel Robert Mueller.

At the center of the case was Stone’s quest in the months leading up to the 2016 presidential election to obtain the emails from WikiLeaks stolen by Russian Main Intelligence Directorate (GRU) operatives from the Democratic National Committee and people within Hillary Clinton’s presidential campaign organization. Stone frequently bragged about his connections with WikiLeaks’ Julian Assange, and Stone communicated with the Trump campaign about WikiLeaks’ plans to release those emails “every chance he got,” said lead federal prosecutor Jonathan Kravis.

Stone was found to have concealed the nature of his communications with WikiLeaks and to have lied to Congress about who acted on his behalf in those contacts. And he attempted to dissuade one of those intermediaries, radio personality Randy Credico, from contradicting his false testimony to Congress, making *Godfather II* references in his messages to Credico—threatening to take away his therapy dog and to order his lawyers to “rip you to shreds.” At one point, Stone allegedly even texted Credico, “Prepare to die [expletive].”

Stone communicated these threats and other details over

WhatsApp, which he used as a “secure” phone line and for messaging. Because of his weak understanding of WhatsApp, he believed that using the messaging platform would protect his communications from the eyes of investigators. It didn’t, as those who received the messages showed them to investigators. Stone also communicated about his activities heavily through emails, which investigators obtained. Stone then lied to Congress about said activities.

During the trial, deputy chairman of the Trump campaign, Rick Gates, testified regarding a July 2016 phone call between Stone and Trump on the heels of WikiLeaks’ release of emails from Clinton campaign officials. Gates said that as soon as he completed the call with Stone, Trump announced that “more information” would be coming—a reference to future WikiLeaks releases. (Trump’s written response to questions from the Mueller campaign declared that Trump had no memory of specifics of the 21 phone conversations he had with Stone during the campaign.) Stone had said he never talked about his conversations with his WikiLeaks intermediaries with anyone connected to the Trump campaign.

After his indictment, Stone was banned by Judge Amy Berman Jackson from using social media after he posted a photo of Judge Jackson in crosshairs on his Instagram account. Stone had been banned from Twitter after inflammatory posts in 2017. Stone violated Judge Jackson’s order 11 times since February.

https://arstechnica.com/?p=1602575

FCC sued by dozens of cities

after voting to kill local fees and rules



reader comments

49 with 40 posters participating

Share this story

The Federal Communications Commission faces a legal battle against dozens of cities from across the United States, which sued the FCC to stop an order that preempts local fees and regulation of cable-broadband networks.

The cities filed lawsuits in response to the FCC's August 1 vote that limits the fees municipalities can charge cable companies and prohibits cities and towns from regulating broadband services offered over cable networks.

“At least 46 cities are asking federal appeals courts to undo an FCC order they argue will force them to raise taxes or cut spending on local media services, including channels that schools, governments, and the general public can use for programming,” Bloomberg Law wrote Tuesday.

Various lawsuits were filed against the FCC between August and the end of October, and Bloomberg’s report said that most of the suits are being consolidated into a single case in the US Court of Appeals for the 9th Circuit. An FCC motion to transfer the case to the 6th Circuit, which has decided previous cases on the same topic, is pending.

The 9th Circuit case was initially filed by Eugene, Oregon, which said the FCC order was arbitrary and capricious and that it violated the Administrative Procedure Act, the Constitution, and the Communications Act. The cities’ arguments and the FCC’s defense will be fleshed out more in future briefs.

Big cities such as Los Angeles, Chicago, Philadelphia, San Antonio, San Francisco, Denver, and Boston are among those suing the FCC. Also suing are other municipalities from Maine, Pennsylvania, Delaware, Virginia, Maryland, Georgia, Indiana, Iowa, Minnesota, South Dakota, Nebraska, Oklahoma, Texas, Arizona, California, Oregon, and Washington, according to a Bloomberg graphic. The state of Hawaii is also suing the FCC, and New York City is supporting the lawsuit against the FCC as an intervening party.

FCC lost net neutrality preemption battle

Chairman Ajit Pai’s FCC already lost one attempt to preempt local regulation throughout the country. When it repealed federal net neutrality rules, the FCC also preempted states from imposing net neutrality laws. While a federal appeals

court upheld the repeal of the US-wide regulations, it ruled that the FCC can't preempt all state laws in one fell swoop. The state of Washington continues to enforce its net neutrality law, and other states may do so in the future.

The FCC lost its preemption battle on net neutrality largely because it had given up its primary authority to regulate broadband. "[I]n any area where the Commission lacks the authority to regulate, it equally lacks the power to preempt state law," the appeals court ruling in that case said.

When the FCC preempted local cable regulation, a consumer advocate pointed out a similarity with the net neutrality case. The cable decision "is consistent with the commission's current perplexing view that it has no statutory authority over broadband but can nevertheless preempt states and local authorities from exercising their own authority," John Bergmayer, legal director of consumer advocacy group Public Knowledge, said after the August 1 vote.

The FCC argues that states and localities cannot collect fees and impose requirements that aren't explicitly allowed by Title VI, the cable-regulation section that Congress added to communications law with the Cable Act of 1984. The FCC acted partly in response to an Oregon State Supreme Court decision that upheld a 7% "telecommunications" license fee the city of Eugene imposed on Comcast. The FCC wants to get that fee and others off the books.

The US cable law prevents local authorities from collecting more than 5% of a cable operator's gross revenue in any 12-month period. The FCC said that some local governments have been requiring in-kind contributions from cable operators to get around the 5% cap and ruled that most in-kind contributions must count toward that cap.

Pai claimed that the preemption will spur companies to expand broadband networks, but Democratic FCC Commissioner Jessica

Rosenworcel pointed out that ISPs haven't actually promised to deploy more broadband in exchange for the regulatory favor from the FCC. She added that "there is no enforceable obligation to expand broadband capacity."

Five groups representing local governments detailed some of the arguments against the preemption in a filing with the FCC last month. They argued, among other things, that the FCC "has exceeded its authority, inserting itself where Congress provided no authority or direction to do so in a manner contrary to the clear and unambiguous terms of the Cable Act." The local-government groups also said the FCC order violates the 10th Amendment by overriding states' rights, specifically by "directing state and local governments to surrender their property and management rights to 'advance… federal policies' related to broadband deployment."

Local governments also say the FCC order will make it harder to provide public, educational, and government access (PEG) programming. More generally, they say the FCC has "commandeered" the municipalities' "budgets and other resources… for the purpose of compensating cable operators in violation of legitimately adopted local franchises and state laws."

Separately, the FCC is facing another lawsuit filed by cities over the federal agency's September 2018 decision to preempt about $2 billion worth of fees related to deployment of wireless equipment such as small cells used for 5G.

https://arstechnica.com/?p=1602185

FTC head asks Congress for real privacy laws he can enforce



Enlarge / FTC Chairman Joseph Simons testifying about antitrust matters before a Senate committee in September 2019.

reader comments

18 with 18 posters participating

Share this story

In testimony before a House subcommittee Wednesday, Federal Trade Commission Chairman Joseph Simons renewed his call for Congress to pass new privacy legislation, telling representatives, essentially, he can't enforce a law that doesn't exist.

Simons was on Capitol Hill testifying in a hearing on “Online Platforms and Market Power,” the probe the House Antitrust subcommittee launched in June to dig into Apple, Amazon, Facebook, and Google.

At the highest level, the FTC is responsible for basically two things: protecting competition and protecting consumers. To that end, it’s one of the two bodies with antitrust oversight, sharing responsibility with the Justice Department for reviewing mergers and challenging anticompetitive behavior.

As part of the consumer protection half of its mandate, the FTC also regulates the gulf between what companies say they will do and what they actually do. As such, the agency has become the closest thing the United States has to a privacy regulator. But its actions and authority are limited under the law, and when it comes to privacy, the commission can more or less only intervene when a prior agreement has been broken—it can’t just impose fines or other penalties for behavior that feels like it should be illegal but isn’t.

During the hearing, Rep. Joe Neguse (D-Colo.) pressed Simons on the FTC’s track record with privacy enforcement. “I want to talk briefly about the settlement with Facebook earlier this year,” Neguse said, asking Simons to explain the “methodology” the commission used to reach the $5 billion agreement.

“I’m very disappointed that you all are disappointed” in the settlement, Simons replied, defending the settlement as “very aggressive.” But, he added: “Even if we wanted to do more, we don’t have the authority to do more. We do not have the authority to impose fines or, on our own, increase the injunctive relief. We have to go to court. So what we did is we negotiated very long and hard with Facebook to get the best relief we could in a settlement and then compare that to what we would have gotten if we had gone to court.”

Neguse cut Simons off there, but he added, “Ultimately, one

point that I think we both agree on is that the tools that the FTC has under existing statute, in my view, could be strengthened, given the trend and the challenges that your agency faces." Simons agreed.

Later in the hearing, Simons reiterated the sentiment, telling the chamber, "I think if you want us to do more on the privacy front, then we need help from you," Simons said. "We've done as much as we can do with the tools we have."

A frequent refrain

Simons has rung the alarm about this particular enforcement gap several times already this year. The FTC in July announced not only the Facebook settlement but also a $575 million settlement with Equifax over its massive consumer data breach. With each announcement, Simons called on Congress to act.

"The CFPB and the states were able to obtain civil penalties for this massive breach by a major financial institution. The FTC could not," Simons said in a press conference about the Equifax case. "Fortunately other agencies were able to fill in the gap this time. That will not always be the case, which sends the wrong signal regarding deterrence."

During a separate press event about Facebook a week later, he echoed the sentiment, saying "We are a law enforcement agency without the authority to promulgate general privacy regulations. Our authority in this case comes from a 100-year-old statute that was never intended to deal with privacy issues like the ones that we address today."

Members of Congress likewise have been calling on their colleagues to do something about federal privacy laws. Sen. Ron Wyden (D-Ore.) last month proposed a bill that would not only drastically expand the FTC's scope and resources but also would impose criminal penalties for company officers found responsible for mishandling consumer data.

The House has likewise taken up the call: this month, Reps. Anna Eshoo and Zoe Lofgren, both Democrats from California, introduced an Online Privacy Act earlier this month. Their bill would not only create new standards but also take their enforcement out of the hands of the FTC altogether, instead creating a Digital Privacy Agency to handle it.

In the meantime, regulators have been doing the best they can to consider whether matters of consumer data and privacy fall under antitrust law. DOJ antitrust chief Makan Delrahim has several times discussed ways in which poor privacy controls that harm consumers may be considered a result of poor competition.

“As a foundational matter, we must acknowledge that data has economic value, and some observers have said it is analogous to a new currency,” Delrahim said in a speech last week:

> *Like other features that make a service appealing to a particular consumer, privacy is an important dimension of quality. For example, robust competition can spur companies to offer more or better privacy protections. Without competition, a dominant firm can more easily reduce quality—such as by decreasing privacy protections—without losing a significant number of users.*
>
> *As I have said before, these non-price dimensions of competition deserve our attention and renewed focus in the digital marketplace.*

https://arstechnica.com/?p=1602063