Trump vows not to extend TikTok deadline beyond September 15

Enlarge / Trump speaks at Andrews Air Force Base on September 10, 2020, before boarding a flight for a campaign rally in Michigan.
MANDEL NGAN/AFP via Getty Images

reader comments

94 with 56 posters participating

Share this story

ByteDance, the Chinese company that owns TikTok, is facing a looming September 15 deadline to sell its US operations or have them shut down by the Trump administration. On Thursday evening, President Trump told reporters that the deadline wouldn't be pushed back.

"We'll either close up TikTok in this country for security reasons, or it'll be sold," Trump said just before boarding a flight to Michigan. "I'm not extending deadlines. No. It's September 15. There will be no extension of the TikTok deadline."

Reports indicate that both Microsoft and Oracle have made offers for ByteDance's US operations. The problem is that the companies may not be able to appease the conflicting demands of the US and Chinese governments.

In early August, Trump declared TikTok a national security threat due to the potential for the Chinese government to

collect data on American users and to conduct disinformation campaigns in the United States. Trump claimed that the International Emergency Economic Powers Act gives the president the authority to shut down an app like TikTok if it threatens national security.

A follow-up order on August 14 retroactively blocked ByteDance's 2017 acquisition of Musical.ly, the platform that subsequently evolved into TikTok. The president has the power to block international mergers that raise national security concerns, and some experts see this as a stronger legal basis for shutting down the service.

ByteDance fielded offers from both Microsoft and Oracle and was reportedly close to choosing one of them when the Chinese government intervened. At the end of August, Beijing announced new export control rules that limited exports of artificial intelligence software without government approval.

TikTok has sophisticated video recommendation algorithms that would likely run afoul of those rules. So the new rules mean that any sale would have to be approved by the Chinese government—which would prefer not to have the US seize control of one of China's most popular global technology platforms.

There's a danger that the conflicting demands of the US and Chinese governments will leave no room for TikTok to do a deal with Microsoft, Oracle, or anyone else. In that case, ByteDance might be forced to shut down its US operations.

But it's not clear when a ban would actually take effect. Trump has told reporters that ByteDance needs to do a deal by September 15. But Trump's written executive orders gave different deadlines: around September 20 for the first executive order and mid-November for the second one. These deadlines could also be pushed back by the courts as they consider ByteDance's arguments that the orders themselves are illegal.

https://arstechnica.com/?p=1705274

Revisiting the spectacular failure that was the Bill Gates deposition

Aurich Lawson

reader comments

116 with 79 posters participating

Share this story

When Microsoft backed a key motion filed two weeks ago in Epic Games' antitrust lawsuit against Apple, it raised a few eyebrows.

Two decades ago, the US Justice Department, 18 states, and the District of Columbia sued Microsoft on allegations the Windows operating system represented a monopoly that the company was wielding to prop up its then fledgling Internet Explorer browser, in violation of the Sherman Antitrust Act of 1890. The suit expressly claimed that Microsoft was using Windows to freeze out the Netscape browser and, more tacitly, Sun Microsystems' cross-platform Java platform as well.

The software maker vehemently bristled at the allegations and claimed that the action represented a government intrusion brought at the behest of companies that couldn't compete on

the merits. Microsoft warned that the action would set a dangerous precedent that could stifle innovation for years to come.

The company's legal response was one of the most vigorous I've covered in my 25 years as a journalist. The PR campaign reached shock-and-awe proportions, as well, with handlers at one point arranging a poorly executed astro turf campaign intended to galvanize public opinion against the legal action.

Now, in 2020, a Microsoft executive has submitted sworn written testimony in support of plaintiff Epic Games alleging that Apple has a "complete monopoly over the distribution of apps to the billion users of iOS … to coerce app developers into using Apple's payment platform."

The legal declaration, from Microsoft Gaming Developer Experiences General Manager Kevin Gammill, came in response to Apple's threat to deny Epic access to software development tools it needed to develop its Unreal Engine game platform for use on iOS. Apple made the threat after Epic tried to use its own payment system in the iOS version of *Fortnite* to get around Apple's 30-percent platform fee. That move quickly got the game pulled from the Apple App Store and led Epic to file a lawsuit in response.

Gammill said that any move harming development of Epic's Unreal Engine on iOS would hurt Microsoft's business, because "in Microsoft's view there are very few other options available for creators to license with as many features and as much functionality as Unreal Engine across multiple platforms, including iOS."

Role reversal

While Microsoft's filing expressed no opinion on the underlying antitrust claims, the declaration nonetheless illustrated a dramatic about-face for a company culture that

once wore its contempt for antitrust law and theory on its sleeve. No longer the Goliath it once was—in large part because of the ascendance of companies like Google, Facebook, and Apple made possible by a settlement Microsoft signed—Microsoft was now comfortable supporting the Davids of the tech industry.

The August filing also represented a major reversal of another sort. In the mid to late 1990s when the events leading to the antitrust suit were playing out, Apple was on life support. Microsoft knew this, and according to the government suit, the company used the maker of Macs as a pawn in a bid to blunt the threat Navigator and Java posed to the Windows monopoly. Now, Apple represents the Goliath Microsoft was helping to slay.

All of this got me thinking about the one of the most memorable parts of my coverage of Microsoft antitrust trial—the videotaped deposition of Bill Gates, the company's cofounder and at the time its CEO and chairman. At its most basic level, the deposition underscored the utter contempt he had for an action he believed impinged the ability of his company—and others to follow, he warned—to design products and conduct business as they saw fit.

The strategy during the three-day deposition was classic Microsoft. Obstruct. Paint the government as out-of-touch policy wonks who had no idea how tech and real markets worked. And above all, deny even the most basic of premises in the government's case. The plan from Gates' army of lawyers and PR handlers seemed to be to wield his image as a software wunderkind who dropped out of Harvard to bootstrap his company and went on to become the world's richest man. Team Gates planned to use that same domineering force of will to beat back government lawyers.

A spectacular failure

By day 2, it became clear that strategy was failing spectacularly. As New Yorker writer Ken Auletta once noted, Gates had never in his life groveled for a job or suffered many of the indignities most of us experience on a regular basis. He regularly berated reporters for asking what he'd say were stupid questions. Publicly lauded as the wise sage, consummate businessman, and industry visionary, Gates was accustomed to being treated with obsequious deference from all but a small number of peers. As such, he had little or no experience tolerating—let alone encountering—dissent, criticism, or challenges to his authority.

The lack of experience played right into the government's hand. Instead of portraying a leader in control of his domain and confident in his case and his company's legal and ethical righteousness, the courtroom videos showed a side of Gates that had never been on public display before. He was petulant, petty, flustered, and dour. He was ineffectual. He was, in a word, beaten.

During three days of intense questioning, Gates often feigned ignorance of his own company's policies and actions. He parsed everyday words or phrases such as "concern," "support," and "piss on." Gates seemed to use the strategy to evade tough questions about whether his company abused its entrenched Windows franchise to kill off emerging competitors, such as Navigator and Java. To the surprise of him and his many attorneys and image handlers, Gates came off as argumentative, petty, and someone badly losing ground to a more formidable rival.

One example came in this exchange with David Boies, the private attorney hired by the Justice Department:

> ***Boies:*** *What non-Microsoft browsers were you concerned about in January of 1996?*

Gates: *I don’t know what you mean “concerned.”*

Boies: *What is it about the word “concerned” that you don’t understand?*

Gates: *I’m not sure what you mean by it.*

Boies: *Is—*

Gates: *Is there a document where I use that term?*

Boies: *Is the term “concerned” a term that you’re familiar with in the English language?*

Gates: *Yes.*

Boies: *Does it have a meaning that you’re familiar with?*

Gates: *Yes.*

https://arstechnica.com/?p=1704751

AT&T hopes you’ll forget its years-long fight against accurate broadband maps

Enlarge / AT&T’s logo at its corporate headquarters on March 13, 2020 in Dallas, Texas.

reader comments

80 with 62 posters participating

Share this story

AT&T—which has spent the past decade fighting US-government attempts to improve the country's horrible broadband maps—is now claiming to be very concerned about the mapping problem that has helped thwart efforts to wire up millions of American homes without adequate broadband access.

AT&T CEO John Stankey this week published an opinion piece in Politico with the apparent goals of improving AT&T's reputation, reducing government regulation, and getting more federal funding. The piece is titled, "A Game Plan to—Finally—Connect Every American to Broadband," and the first item on AT&T's game plan is "to identify where broadband is unavailable with geographic precision."

Stankey wrote:

> *We need to telescope our broadband maps from the macro, census-block level to the micro, building level to understand with more precision where broadband is unavailable. The government's existing mapping methodology is past its shelf life. Currently, it does not identify the exact number and location of households that do not have meaningful broadband service, especially in rural areas. Congress recognized this in March by passing the Broadband DATA Act, which will create a more accurate and detailed map of broadband availability, helping companies like mine have the information needed to determine the focus and cost of deployment. The only problem is that Congress hasn't yet appropriated the funds for the more granular maps, although legislation is currently pending.*

AT&T's years-long fight against

better maps

Why doesn't the United States already have broadband maps with this level of precision? Partly because AT&T and other ISPs have repeatedly fought the Federal Communications Commission's attempts to require submission of more accurate maps.

AT&T may have recognized that its fight against more accurate broadband maps is largely over, with Stankey's Politico essay noting Congress' passage of the Broadband DATA Act—and urging Congress to hurry up in appropriating funding. But even with the Broadband DATA Act mentioned by Stankey, AT&T is still pushing for limits on how the FCC implements the data-collection system mandated by Congress.

Here are some examples from AT&T's filings to the FCC since 2011:

- In April 2011, AT&T told the FCC that ISPs shouldn't have to report the street addresses where they've deployed broadband to homes and should not be required "to report actual broadband speeds." AT&T also said the FCC should not collect data on broadband prices, service quality, or customer satisfaction.
- In February 2013, AT&T met with FCC officials to discuss how collecting more accurate broadband data would "impose new burdens on AT&T" because "the information is not gathered in the course of its normal business operations."
- In October 2017, AT&T told the FCC that "the Commission's proposal to collect mobile broadband and voice subscribership, and fixed broadband deployment at a more granular level, e.g. the sub-census block/address level, should be rejected because it would not generate useful information." Address-level data would not be useful "because providers do not record addresses in a standardized, uniform manner," AT&T said.

- In another October 2017 filing, AT&T said that the FCC should not even give ISPs the *option* of providing geospatial broadband data instead of the less-accurate census-block data ISPs were otherwise required to submit. (The FCC finally required geospatial maps in an August 2019 vote.)

Recognizing that opinion within the government had shifted—with even a prominent Republican senator criticizing FCC Chairman Ajit Pai's failure to deliver more accurate maps—AT&T in October 2018 conceded that more accurate data was necessary and offered its own proposal for collecting it.

Despite that change, AT&T continued pushing for limits on mapping requirements:

- In September 2019, AT&T told the FCC that "transparency" around how ISPs use radio-propagation models to generate maps would be preferable to "more prescriptive standards."
- In October 2019, AT&T said the FCC should not demand more accurate 5G maps, saying that "requiring 5G coverage maps in this early stage of 5G deployment could reveal sensitive information about cell site locations and even customer locations, in cases where 5G is being deployed in high-band spectrum for specific enterprise customers." AT&T also pushed for limits on requirements for reporting the speed of non-5G networks.
- In July 2020, AT&T objected to the FCC's proposal for implementing the Broadband DATA Act, saying that "many" of the data points the FCC proposed requiring are "of questionable value" or unnecessary for verifying the accuracy of carrier-submitted coverage maps.
- In August 2020, AT&T objected to the FCC's proposal to require drive tests to verify the accuracy of mobile-coverage maps, complaining that it would be "simply too costly especially at a time when investment in 5G deployment is a top national priority."

- On September 8, 2020, the same day Stankey's essay in Politico was published, AT&T told the FCC that the agency should not require additional details to verify the accuracy of propagation models used by mobile carriers to generate coverage maps. AT&T also said the FCC "should not require providers to submit additional coverage maps based on different speed thresholds, cell edge probability or cell loading factors."

The FCC, which is still finalizing its plan, has good reason to ask for more data to verify carrier submissions. In April, AT&T admitted a mistake in which it falsely reported offering broadband in nearly 3,600 census blocks spread across parts of 20 states. Separately, the FCC found in December that Verizon, T-Mobile, and US Cellular exaggerated their 4G coverage in official filings. These types of mistakes can prevent the FCC from targeting funding to the areas where it's most needed, and inaccurate data in general can result in ISPs giving potential customers false information about service availability.

More money, please

Besides mapping, other items in Stankey's game plan could result in the broadband industry getting more money. Stankey noted that "Millions of American families cannot afford or may lack access to" high-speed broadband and that the "homework gap" has left many low-income, minority, and rural students without adequate connectivity.

"Market forces and private companies can't do it alone because of the lack of return on the significant investment necessary to reach all Americans," Stankey wrote.

AT&T's targeting of the most profitable areas has left millions of homes in its 21-state service area without adequate broadband access. AT&T doesn't want to bring fiber to all those homes that still have copper phone lines, and

Stankey thus urged Congress to appropriate broadband funding that would allow fixed wireless access instead of fiber in unserved rural areas.

"[A]s Congress debates earmarking up to $80 billion for rural broadband as part of the next round of pandemic relief, we should give equal weight to wired and wireless options," Stankey wrote. He also urged the government to avoid "unnecessary regulations [that] will make greater private sector investment less sustainable." If the United States fails to close its broadband gaps, the fault will lie with the government, not private industry, according to Stankey:

> *With so many students having to learn virtually this fall, and with so many workers now dependent on home Internet connections to keep their jobs, now is the time for us to work together to ensure all American families have access to critical connectivity and the resources needed to meet the urgent challenges of today and tomorrow. If policymakers fail to act, today's "homework gap" will not only exacerbate the proverbial "generation gap," but we will have failed to bridge it.*

AT&T has gotten numerous government favors in the Trump era, such as the repeal of net neutrality rules, deregulation of the broadband industry, and a big corporate tax cut. AT&T's then-CEO Randall Stephenson claimed in November 2017 that AT&T would use a tax cut to create "7,000 jobs of people putting fiber in ground," but AT&T has since laid off tens of thousands of workers and reduced network spending.

Consumer advocates agree that government should promote broadband deployment, but they propose something more ambitious than AT&T's call for more funding and less regulation. Noting that big ISPs "fail to deliver universal access but enjoy comfortable monopolies and charge you prices at 200 percent to 300 percent above competitive rates,"

Electronic Frontier Foundation Senior Legislative Counsel Ernesto Falcon recently wrote in support of a nationwide fiber plan proposed by Democrats:

> *Even when it is profitable to deliver fiber, the national ISPs have chosen not to do it in exchange for short-term profits. A massive infrastructure program, the kind that helped countries like South Korea become global leaders in broadband, aren't just desperately needed in the United States, it is a requirement. No other country on planet Earth has made progress in delivering universal fiber without an infrastructure policy of this type.*

https://arstechnica.com/?p=1705038

Climate change may wreck economy unless we act soon, federal report warns

Enlarge / A boat motors by as the Bidwell Bar Bridge is surrounded by fire in Lake Oroville during the Bear fire in Oroville, California, on September 9, 2020.

reader comments

140 with 105 posters participating

Share this story

The ever-worsening climate crisis is already causing waves of human suffering—both internationally and here in the United States. And now, a new report from a US financial regulator finds that climate change is also poised to do major damage to some of the institutions with the most power to help mitigate it: Wall Street banks and investors.

Climate change "poses a major risk to the stability of the US financial system and to its ability to sustain the American economy," the report (196-page PDF) from the US Commodity Futures Trading Commission (CFTC) begins. Regulators "must recognize that climate change poses serious emerging risks to the US financial system, and they should move urgently and decisively to measure, understand, and address these risks."

The report, called "Managing Climate Risk in the US Financial System," was written by a group of 35 advisors from major banks such as Morgan Stanley and JPMorgan Chase, environmental groups such as The Nature Conservancy and Ceres, energy firms such as BP and ConocoPhillips, several investment firms, and experts from several universities. It is the first analysis of climate change to come from a US financial regulator looking specifically at how change, already underway, will affect trading of agricultural commodities and futures, the real estate and insurance markets, and all the complex financial instruments that are built on multiple industries taken together.

Climate change is already affecting financial markets, real estate, insurance, and infrastructure, the authors find. They conclude that if the US economy is going to survive, we need to first and foremost put a realistic, literal financial cost on the social toll of carbon emissions. Everything else can flow from there.

Growing costs, hard to predict

It is “no longer theoretical” that climate change will produce costly events, the report says, citing the combinations of hurricanes and wildfires that struck the United States in 2018 and 2019. The financial risks of such disasters are also real, and they grow throughout a system.

The report was commissioned by the agency that deals with commodities and futures, so the authors take time to examine what the market has or has not appropriately considered. Unfortunately, they find that present-day markets, such as they are, are basically ignoring climate change.

“Evidence is accumulating that markets are pricing in climate-related risks imperfectly, and sometimes not at all,” the report says, adding that studies have found “no association between current stock prices and measures of predicted changes in climate-related physical hazards.”

In other words: investors and businesses are carrying on as if nothing is changing, when in fact everything is. And if those financial institutions want to avoid “larger exposures to risky assets” than they want to have—and, for that matter, “disruption or impairment of all or part of the financial system”—that’s going to have to change.

Mitigation

The best way to go forward, the authors conclude, may be by going slightly backward and getting the United States back on board with the landmark international Paris Agreement to limit greenhouse gases.

The Trump administration pulled the US out of the Paris Agreement in 2017, and the withdrawal became official in 2019. But in order to mitigate climate change, the US—through Congress—needs to adopt a carbon pricing scheme that is “fair,

economy-wide, and effective in reducing emissions consistent with the Paris Agreement.”

All the Federal financial regulators, including the Federal Reserve and the Securities and Exchange Commission, also need to “incorporate climate-related risks” into their mandates, analyses, and work, the report adds. The consideration of climate-related risk should persist at every level, including strategic planning and organizational structure, and agencies should put time and effort into researching the potential and likely financial implications—both systemic and sub-systemic—of climate risks.

The United States also can’t go it alone, the report finds, calling on US regulators to “actively engage their international counterparts to exchange information and draw lessons on emerging good practice” in how to handle climate-related risks.

Getting the US to change, however, is likely to be an uphill battle at least in the short term. The Trump administration has been on a deregulatory tear since 2017, killing off vehicle fuel efficiency rules, methane emissions rules, and a slew of other environmental regulations. Neither is Congress particularly inclined to act on anything at this moment in time, particularly not when it comes to crafting complex new legislation. This may or may not change in 2021, depending on the outcomes of the impending national election.

https://arstechnica.com/?p=1704657

Trump audio shows he knew about COVID’s severity even as he misled public

reader comments

483 with 189 posters participating

Share this story

On February 7 this year, President Donald Trump admitted in an interview with journalist Bob Woodward that the coronavirus was far more deadly than the flu even as Trump continued misleading the public about the pandemic’s severity. In another interview on March 19, Trump told Woodward that he was intentionally downplaying the virus’s severity. “I wanted to always play it down,” Trump said.

Woodward’s new book, *Rage*, is scheduled for release next week, but excerpts of the book along with recordings of Trump’s interviews with Woodward became public today. This CNN article contains several audio clips from the interviews.

The audio excerpts came from 18 interviews between December 5, 2019 and July 21, 2020 that “were recorded by Woodward with Trump’s permission,” CNN wrote. In the February 7 interview, Trump noted that the flu kills 25,000 or 30,000 people a year in the United States. “This is more deadly,” Trump then told Woodward, referring to the coronavirus. (So far, about 190,000 Americans have died from COVID-19.)

Enlarge / The cover of Bob Woodward’s book about President Trump, titled *Rage.*

“It goes through air, Bob,” Trump said. “That’s always tougher than the touch. You know, the touch, you don’t have to touch things. Right? But the air, you just breathe the air and that’s how it’s passed.” The coronavirus is “more deadly than… even your strenuous flus,” Trump added.

As CNN noted, that February 7 interview came 10 days after a “top-secret intelligence briefing” in which “National Security Advisor Robert O’Brien gave Trump a ‘jarring’ warning about the virus, telling the President it would be the ‘biggest national security threat’ of his presidency. Trump’s head ‘popped up,’ Woodward writes.”

Deputy National Security Advisor Matt Pottinger reportedly then warned Trump that the coronavirus could be as bad as the flu pandemic of 1918 that killed about 50 million people worldwide including 675,000 in the United States.

Trump in public: It’s “the same as the flu”

Publicly, Trump continued to compare the coronavirus to the seasonal flu. “View this the same as the flu. When someone sneezes, I try and bail out as much as possible with the sneezing,” Trump said in a February 27 news conference. “Whatever happens, we’re totally prepared,” he said at another point in that news conference.

Trump’s coronavirus/flu comparisons continued in a March 9 tweet. “So last year 37,000 Americans died from the common Flu. It averages between 27,000 and 70,000 per year. Nothing is shut down, life & the economy go on. At this moment there are 546 confirmed cases of CoronaVirus, with 22 deaths. Think about that!” Trump wrote.

Later that week, National Institute of Allergy and Infectious Diseases Director Anthony Fauci told Congress that COVID-19 “is 10 times more lethal than the seasonal flu” and that “it’s going to get worse.”

Trump continued his flu comparisons on March 24, saying in a Fox News virtual town hall that “We’ve had horrible flus… but we’ve never closed down the country for the flu. So you say to yourself, ‘What is this all about?'”

Trump finally acknowledged publicly on March 31 that “It’s not the flu. It’s vicious.”

Trump: “I still like playing it down”

In the March 19 interview with Woodward, Trump explained why he continually downplayed the coronavirus’ severity. “Well I think, Bob, really, to be honest with you, I wanted to always play it down. I still like playing it down, because I don’t

want to create a panic," he said.

In a briefing with reporters today, White House Press Secretary Kayleigh McEnany denied that Trump intentionally misled the public about COVID—even though Trump is on tape saying "I still like playing it down."

"The president has never lied to the American public on COVID," McEnany said. "The president was expressing calm and his actions reflect that."

In the March 19 interview, Trump said the virus was affecting both young and old people. "Just today and yesterday, some startling facts came out. It's not just old, older. Young people too, plenty of young people," Trump told Woodward at the time, according to CNN's summary of the book.

Publicly, Trump claimed in August that children "are virtually immune from this problem." (The CDC says children are less likely to develop serious illness from COVID-19 than adults but stresses that "children are still at risk of developing severe illness and complications from COVID-19.")

Fauci calls Trump's attention span a "minus number"

For months, Trump has claimed that the virus would simply "disappear" like a "miracle" or "go away." Yet on April 5, two days after one such public statement that the virus "is going away," Trump told Woodward, "[I]t's a horrible thing. It's unbelievable." On April 13, Trump told Woodward that "it's so easily transmissible, you wouldn't even believe it."

Just as he has in public, Trump insisted in interviews with Woodward that the virus's spread in the United States wasn't his fault. "The virus has nothing to do with me," Trump told Woodward in July, according to CNN. "It's not my fault. It's—China let the damn virus out."

The book also includes quotes about Trump from government officials. According to CNN, Woodward quotes Fauci as telling other people that Trump's leadership is "rudderless," that his "attention span is like a minus number," and that "his sole purpose is to get reelected."

Listing image by Simon & Schuster

https://arstechnica.com/?p=1704720

Pentagon's review of controversial $10B contract was a sham, Amazon claims

Enlarge / The Pentagon in its natural habitat—Arlington, Virginia—in 2018.

reader comments

87 with 65 posters participating

Share this story

Amazon is continuing to fight the Department of Defense over a $10 billion contract, as the Pentagon has completed its review of the deal and determined once again that it was correct to award the entire project to Microsoft.

The DOD launched bidding for the Joint Enterprise Defense Infrastructure (JEDI) project, a massive cloud-computing

contract, in 2019. By April of that year, the shortlist was down to two finalists: Amazon AWS and Microsoft Azure. Amazon was widely considered the favorite, and many industry watchers expressed surprise when Microsoft ultimately landed the deal in October 2019.

Amazon filed suit, alleging that the decision was politically motivated and quoting President Donald Trump's alleged intention to "screw Amazon." In February of this year, a federal judge agreed to order an injunction on the deal pending the outcome of the case.

The DOD launched its own initial investigation of the contract process. That review, which concluded in April, determined that the DOD did nothing wrong in awarding the contract to Microsoft—even though the White House stonewalled investigators and refused to provide witnesses for the probe.

The agency this spring also launched a reconsideration of specific parts of the contract. That review concluded just before the Labor Day holiday weekend, with the Pentagon reaffirming that "Microsoft's proposal continues to represent the best deal to the government." Work on the contract, however, cannot begin while the injunction is in place.

Microsoft applauded the DOD's decision. "We appreciate that after careful review, the DoD confirmed that we offered the right technology and the best value," the company said in a statement. "We're ready to get to work and make sure that those who serve our country have access to this much needed technology."

Amazon, in a scathing corporate blog post, strongly rejected the agency's findings.

"Taking corrective action should have provided the DOD an opportunity to address the numerous material evaluation errors outlined in our protest, ensure a fair and level playing field, and ultimately, expedite the conclusion of litigation,"

Amazon wrote. “Unfortunately, the DOD rejected that opportunity.”

Amazon’s bid for JEDI came in “tens of millions of dollars” lower than Microsoft’s, the company alleges, and the “review” was effectively just for show. Why? Because of President Trump, Amazon says:

> *There is a recurring pattern to the way President Trump behaves when he’s called out for doing something egregious: first he denies doing it, then he looks for ways to push it off to the side, to distract attention from it and delay efforts to investigate it (so people get bored and forget about it). And then he ends up doubling down on the egregious act anyway. On JEDI, President Trump reportedly ordered former Secretary [of Defense James] Mattis to “screw” Amazon, blatantly interfered in an active procurement, directed his subordinate to conduct an unorthodox “review” prior to a contract award announcement and then stonewalled an investigation into his own political interference. “Corrective action” was used as a way to halt our litigation, delay further investigations and incorrectly give the appearance that only one issue needed to be fixed while giving the impression that the DoD was actually going to fix something… This corrective action changed nothing, wasted five months that could have been spent getting to the bottom of these serious concerns, and was designed solely to distract from our broader concerns and reaffirm a decision that was corrupted by the President’s self-interest.*

Amazon intends to keep pursuing its legal action against the Department of Defense, the company added.

https://arstechnica.com/?p=1704497

China plans new data policy in response to Trump admin’s “bullying”

Enlarge / The tech trade war between China and the US just keeps on escalating.

reader comments

119 with 78 posters participating

Share this story

China’s government today unveiled a new data-security initiative in response to the Trump administration’s efforts to cut Chinese hardware and software out of the US tech scene.

“It is important to develop a set of international rules on data security that reflect the will and respect the interests of all countries,” China Foreign Minister Wang Yi said, according to Bloomberg’s and The Wall Street Journal‘s reads of the announcement (link is in Chinese).

Wang in his remarks said China is willing to contribute its “wisdom” to building a framework, in which participating countries would handle data security in a “comprehensive, objective and evidence-based manner” to maintain “open, secure and stable global supply chains.” The suggested policy would also forbid governments from accessing data acquired by firms’ overseas operations—basically, what happens in China stays in China and doesn’t get shared with US authorities.

Trade War! USA v. China

View more stories

The move by China's government follows the US State Department's Clean Networks purge. Under the Clean Network guidance, the administration is explicitly prohibiting Chinese technologies from US mobile networks, US mobile app stores, and US cloud computing applications.

Chinese companies "pose a danger to US national security and should not provide international telecommunications services to and from the United States," Secretary of State Mike Pompeo wrote in the August announcement. Apps from China "threaten our privacy, proliferate viruses, and spread propaganda and disinformation. American's [sic] most sensitive personal and business information must be protected on their mobile phones from exploitation and theft for the CCP's benefit," Pompeo added.

Wang did not specifically name the United States in his remarks, but he did allude very clearly to the administration's policies. "Bent on unilateral acts, a certain country keeps making groundless accusations against others in the name of 'clean' network and used security as a pretext to prey on enterprises of other countries who have a competitive edge," he said. "Such blatant acts of bullying must be opposed and rejected."

Tick… tock… tick… tock…

The administration's years-long actions against Chinese firms most recently came to a head when President Trump declared TikTok and WeChat to be national emergencies and issued a pair of executive orders effectively banning them from operating in the United States as of September 15.

TikTok and its parent company, ByteDance, are suing the

administration, arguing that the executive order is unconstitutional and politically driven. Even while the suit is underway, several US firms—including Microsoft, Oracle, and Walmart—are competing to put in bids for TikTok's US operations before next week's deadline hits.

China, however, is moving to counteract that potential sale as well. The Chinese government last week announced new export restrictions for artificial intelligence technology including "such computing and data-processing technologies as text analysis, content recommendation, speech modeling and voice-recognition." That prohibition could cover TikTok's recommendation engine, which is a large part of its success—and, if so, would make sale to a US firm difficult or perhaps even not possible.

China has always been more restrictive with its citizens' Internet use than the US and has long prohibited access to certain platforms and sites, notably including Facebook. Even so, however, China appears to be ramping up bans on American apps in response to US policy. TechCrunch reports that Scratch, a popular platform developed at MIT on which children can learn to code, has been banned inside China since the middle of August.

https://arstechnica.com/?p=1704383

The FBI botched its DNC hack warning in 2016—but says it

won’t next time

Enlarge / By notifying hacking victims sooner and at higher levels, the FBI hopes to avert another high-impact communications breakdown.
Drew Angerer | Getty Images

reader comments

13 with 12 posters participating

Share this story

On April 28, 2016, an IT tech staffer for the Democratic National Committee named Yared Tamene made a sickening discovery: A notorious Russian hacker group known as Fancy Bear had penetrated a DNC server “at the heart of the network,” as he would later tell the US Senate’s Select Committee on Intelligence. By this point the intruders already had the ability, he said, to delete, alter, or steal data from the network at will. And somehow this breach had come as a terrible surprise—despite an FBI agent’s warning to Tamene of potential Russian hacking over a series of phone calls that had begun fully nine months earlier.

The FBI agent’s warnings had “never used alarming language,” Tamene would tell the Senate committee, and never reached higher than the DNC’s IT director, who dismissed them after a cursory search of the network for signs of foul play. That miscommunication would result in the success of the Kremlin-sponsored hack-and-leak operation that would ultimately contribute to the election of Donald Trump.

Four years later, the FBI and the community of incident response security professionals who often work with the bureau's agents says the FBI has significantly changed how it communicates with hacking victims—the better to avoid another DNC-style debacle. In interviews with WIRED, FBI officials never explicitly admitted to a failure in the case of the DNC's botched notification. But they and their private sector counterparts nonetheless described a bureau that has revamped its practices to warn hacking targets faster, and at a higher level of the targeted organization—especially in cases that might involve the upcoming election or the scourge of ransomware costing companies millions of dollars across the globe.

In December of last year, for instance, the FBI announced a new formal policy of immediately notifying state government officials when the bureau identifies a threat to election infrastructure they control. But the improvements go beyond warnings to state officials, says Mike Herrington, the section chief of the FBI's cyber division. "I see a key change in practice and emphasis, getting our special agents in charge keyed up to gain the full cooperation of potential victims," says Herrington, who says he's personally notified dozens of victims of hacking incidents over his career.

Those "special agents in charge" are higher-ranking than the typical field agents who have notified victims in the past, notes Steven Kelly, the FBI's chief of cyber policy. Kelly says that those special agents have also been instructed to aim their warnings further up the victim's org chart. "We want them to be reaching out to the C-suite level, to senior executives," says Kelly. "To make sure they're aware of what's going on and that they're putting the right amount of calories into addressing the issues so that these things don't get ignored or buried."

First alert

Unlike practically every other crime the FBI deals with, the bureau is often in the strange position of being the first to tell a person or organization that they're victims of a cyberattack. Often the warnings are based on evidence pulled from ongoing hacking campaigns—sometimes from intelligence agencies or even foreign governments—such as a common command-and-control server across different intrusions. "It is often a very significant event in that person's career or life to have the FBI calling them and saying we believe you may be the victim of a crime," Herrington says.

Over the last decade, though, the FBI's role as messenger has shifted, as organizations become more adept at discovering their own intrusions. For the past several years, roughly half of hacker intrusions were discovered by the victims themselves, according to the M-Trends report on data breach responses published by incident response firm Mandiant. That's a drastic change from 2011, when 94 percent of breaches were first detected by an outside organization, usually law enforcement.

Even so, the growth in the sheer number of hacking incidents means the FBI is notifying far more victims than in the past, says Jake Williams, a former NSA hacker and founder of the security consultancy Rendition Infosec, which often acts as an incident response firm for hacking victims. Williams says that in the last few years, he's seen a doubling or tripling of the number of calls that his firm gets from hacking victims who were first notified by the FBI. The notifications still often provide just the bare minimum of information about the breach—such as the FBI's observation that a computer on the victim's network connected to a known malicious server—and victims are expected to call in their own incident response consultants to kick the hackers out, with little assistance from the FBI itself.

But Williams also says he’s found that the bureau now notifies victims sooner after its agents detect a breach; in years past, the FBI would sometimes warn victims only that they had *been* the victim of an intrusion, often well after the fact. “We’re getting more information on the front side,” says Williams. “Before it was commonly, ‘we can’t tell you exactly when and we don’t know if it’s still going on, but you should know.'”

By some accounts, at least, the scandalous failure of communication that allowed Russian hackers to run wild in the DNC’s networks is far less likely to occur today. One DNC official told WIRED that the organization has had regular meetings with FBI agents since 2016; if another incident occurs, the two organizations would already have relationships between senior officials on both sides. “Basically we’ve solved this problem and have really good, clear channels of communication,” the DNC official wrote in an email.

Dmitri Alperovitch, the former CTO of Crowdstrike, which handled the incident response for the DNC’s 2016 breach and many other incidents of state-sponsored hacking, agrees that the FBI’s practices have changed—specifically that it’s taking more care to reach senior executives or officials who will take its warnings seriously. Alperovitch points out that the FBI actually warned the DNC within days of the Russian hackers’ first breaching its network. The problem, he says, was that the agents working the case had settled for a warning to a low-level staffer. “They should have reached out to higher ups,” Alperovitch wrote in a message to WIRED. “I do see them going higher up the chain these days, so yeah, I think it’s better.”

Held for ransom

Elections aside, the epidemic of ransomware hitting US companies has also forced the FBI to improve and accelerate

its warnings to hacking victims. For some of those cases, says special agent Tyson Fowler, the FBI has developed a so-called “emergency lead notification” process that bypasses the bureau’s usual internal consultations and immediately notifies a cybersecurity-focused agent in a field office who can warn a victim, hopefully before the hackers deliver their ransomware payload. “We’re leaning forward in terms of notifying victims as soon as possible and skipping all those steps,” says Fowler.

In one case in February, for instance, Fowler says he learned of a ransomware-focused intrusion into a Georgia-based multinational company’s network and, by the end of the day, had reached the CEO of the company to warn about the impending attack. The company took part of its network offline, disrupting the hackers’ access to their malware, Fowler says. “You have what could have been an extinction level event for the company, and we were able to avoid the financial impact and the privacy impact just by the quick response,” says Kevvie Fowler, an incident responder with Deloitte whom the company brought in to help remediate the breach.

None of that renewed urgency in victim notification guarantees that hackers won’t outrun defenders anyway. They may, in fact, be learning to operate faster inside of victim networks as the pace of response quickens. But at least in cases where the FBI gets wind of an ongoing intrusion, the period of free rein they enjoy before being hunted by network responders may no longer last for months, as in the DNC hack, but for days or hours.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1703777

Ajit Pai touted false broadband data despite clear signs it wasn’t accurate

Enlarge / FCC Chairman Ajit Pai and FCC Commissioner Jessica Rosenworcel at a Senate Commerce Committee hearing in Washington, D.C., on Wednesday, June 24, 2020.

reader comments

113 with 78 posters participating

Share this story

Federal Communications Commission Chairman Ajit Pai touted inaccurate broadband-availability data in order to claim that his deregulatory agenda sped up deployment despite clear warning signs that the FCC was relying on false information.

Pai claimed in February 2019 that the number of Americans lacking access to fixed broadband at the FCC benchmark speed of 25Mbps downstream and 3Mbps upstream dropped from 26.1 million people at the end of 2016 to 19.4 million at the end of 2017, and he attributed the improvement to the FCC “removing barriers to infrastructure investment.” The numbers were included in a draft version of the FCC’s congressionally mandated annual broadband assessment, and Pai asked fellow commissioners to approve the report that concluded the broadband industry was doing enough to expand access.

But consumer-advocacy group Free Press subsequently pointed out that the numbers were skewed by an ISP called BarrierFree suddenly “claim[ing] deployment of fiber-to-the-home and fixed wireless services (each at downstream/upstream speeds of

940mbps/880mbps) to census blocks containing nearly 62 million persons." This is an implausible assertion and would have meant BarrierFree went from serving zero people to nearly 20 percent of the US population in just six months. BarrierFree admitted the error when contacted by Ars at the time, saying that "a portion of the submission was parsed incorrectly in the upload process."

Pai corrected the data to acknowledge that 21.3 million Americans still lacked broadband but didn't change his conclusion that broadband was "being deployed to all Americans in a reasonable and timely fashion." (Even that 21.3-million figure was likely an undercount because the FCC counts an entire census block as served even if only one home in the census block can get service.)

This week, the FCC released more details on BarrierFree's apparent history of violating rules requiring ISPs to submit "Form 477" broadband-deployment data every six months, and it shows that numerous warning signs were spotted by FCC staff long before Pai touted the inaccurate data. The FCC on Tuesday issued a Notice of Apparent Liability that proposed a $163,912 fine for BarrierFree, kicking off a process that gives BarrierFree a chance to respond to the allegations and fight the proposed penalty.

Although the FCC is trying to fine BarrierFree for submitting inaccurate data, the commission is not penalizing the ISP for failing to submit over 10 years' worth of required Form 477 reports.

"The Pai FCC slept on BarrierFree's repeated violation of FCC rules," Free Press Research Director Derek Turner told Ars, calling the FCC's attempt to downplay its own role in spreading inaccurate data "shameful."

FCC staff flagged “inaccurate” data in 2018

BarrierFree began serving customers in Suffolk County, New York, in May 2004 but did not submit any of the required Form 477 filings for more than a decade because, it later told the FCC, it thought the filings were voluntary unless an ISP was applying for government grants, the FCC said in the Notice of Apparent Liability.

FCC staff emailed BarrierFree in November 2015, saying that the ISP’s attempt to finally submit a Form 477 report was incomplete and “further action is needed.” FCC staff contacted BarrierFree again in January 2016, saying that “For filings that are valid and remain un-submitted, please keep in mind that your company may be referred to the Enforcement Bureau for non-compliance.”

BarrierFree finally submitted a complete Form 477 filing in March 2018, reporting widespread deployment in Northeast and Mid-Atlantic states despite only serving customers in one part of New York. The filing set off alarm bells among FCC staff for several reasons, such as the ISP claiming that it had more residential broadband connections in one Long Island census tract than the number of actual household units in the tract.

Here’s what happened next, according to the FCC:

> *On June 5, 2018, [FCC] staff notified BarrierFree of “certain items in your filing which are unusual and potentially inaccurate, and corrections may be necessary.” On July 31, 2018, staff repeated that admonition.*
>
> *On July 11, 2018, Commission staff issued a Public Notice reminding Form 477 filers that the next filing would be due no later than September 4, 2018. On August 29, 2018, staff emailed BarrierFree that there was a “FILING DUE DATE APPROACHING.” On September 18, 2018, staff again informed*

> *BarrierFree that "FILING DUE DATE MISSED… POTENTIAL ENFORCEMENT ACTION: Please note that the Commission tracks filers who consistently file Form 477 after the deadline. Failure to file FCC Form 477 in a timely manner may result in fines and penalties." And on October 15, 2018, staff reiterated that admonition.*

BarrierFree did not make the required September 2018 filing, the FCC said. FCC staff sent another warning to BarrierFree on February 19, 2019 about the upcoming March 2019 deadline. Yet on the very same day, the FCC chairman's office issued a press release touting the draft report that included deployment data inflated by BarrierFree's incorrect March 2018 filing. "This report shows that our approach is working," Pai said in the press release.

https://arstechnica.com/?p=1703702

Amazon's top UK reviewers appear to profit from fake 5-star posts

Eric Bangeman

reader comments

137 with 92 posters participating

Share this story

Amazon is investigating the most prolific reviewers on its UK website after a Financial Times investigation found evidence that they were profiting from posting thousands of five-star ratings.

Justin Fryer, the number one-ranked reviewer on Amazon.co.uk, reviewed £15,000 worth of products in August alone, from smartphones to electric scooters to gym equipment, giving his five-star approval on average once every four hours.

Overwhelmingly, those products were from little-known Chinese brands, who often offer to send reviewers products for free in return for positive posts. Mr. Fryer then appears to have sold many of the goods on eBay, making nearly £20,000 since June.

When contacted by the FT, Mr. Fryer denied posting paid-for reviews—before deleting his review history from Amazon's website. Mr. Fryer said the eBay listings, which described products as "unused" and "unopened," were for duplicates.

At least two other top 10-ranked Amazon UK reviewers removed their history after Mr. Fryer. Another prominent reviewer, outside of the top 10, removed his name and reviews and changed his profile picture to display the words "please go away."

The FT's analysis suggested nine of Amazon's current UK top 10 providers of ratings were engaged in suspicious behavior, with huge numbers of five-star reviews of exclusively Chinese products from unknown brands and manufacturers. Many of the same items were seen by the FT in groups and forums offering free products or money in exchange for reviews.

The Competition and Markets Authority, the UK's competition watchdog, launched in May its own probe into online stores over "suspicious" and manipulated reviews, which it estimates influence £23 billion in UK online shopping spend every year.

“We will not hesitate to take further action if we find evidence that the stores aren’t doing what’s required under the law,” a CMA spokeswoman said.

Amazon’s longstanding problem with fake or manipulated reviews appears to have worsened since the coronavirus pandemic turbocharged the number of people shopping on its site. One estimate, from the online review analysis group Fakespot, suggested that the problem peaked in May, when 58 percent of products on Amazon.co.uk were accompanied by seemingly fake reviews.

“The scale of this fraud is amazing,” said Saoud Khalifah, Fakespot’s chief executive. “And Amazon UK has a much higher percentage of fake reviews than the other platforms.”

Amazon said it took such fraud seriously and used AI to spot bad actors, as well as monitoring reports from users. It said it would investigate the FT’s findings.

“We want Amazon customers to shop with confidence knowing that the reviews they read are authentic and relevant,” the company said, adding that it suspends, bans, and sues people who violate its policies.

Justin Fryer’s Amazon review, and an eBay listing for an identical Item sold from his account the day before.
But Amazon has known about the activity on Mr. Fryer’s account since at least early August, when one user of the site emailed chief executive Jeff Bezos directly after his complaints had been ignored.

“Jeff Bezos received your email,” an Amazon employee later replied, pledging to investigate Mr. Fryer and the other high-profile accounts. A number of reviews highlighted were subsequently removed—but no broader action appears to have been taken.

Since February, Mr. Fryer’s reviews from China-based brands have included three gazebos, more than a dozen vacuum cleaners, and 10 laptops—as well as everything from dolls

houses to selfie lights to a “fat removal” machine.

His contributions typically contained a video of the product taken out of its packaging but delicately handled, with comments mostly about the exterior features and the quality of the box it came in. Many of the same products were then listed as “unopened” and “unused” on an eBay account registered under Mr. Fryer’s name and address.

On August 13, for instance, Mr. Fryer sold an electric scooter for £485.99, seven days before posting a review of the same product on Amazon, describing it as “hands down my favourite toy” that he liked “so much we purchased a second one for my fiancée.”

When contacted this week, Mr. Fryer said the items on his eBay listings were duplicates, and that the accusation he was receiving free products in return for positive reviews was “false.” He said he had paid for the “large majority” of goods, but could not say how much he had spent “off the top of his head.”

“I have relationships with and I know some of the sellers,” he said. “My partner’s Chinese and I know a lot of the businesses over there . . . and I just review.”

Unlike bloggers and influencers, who can accept and publicize free products with proper disclosure, Amazon’s community guidelines explicitly prohibit “creating, modifying, or posting content in exchange for compensation of any kind (including free or discounted products) or on behalf of anyone else.”

The exception is the company’s “vine” review program, an invite-only scheme where top reviewers are sent free products that are not contingent on a positive review.

Observers of Amazon’s marketplace say the site’s algorithms greatly incentivize paying for positive reviews, even if it

means doling out expensive products.

Alongside price and delivery time, reviews are a crucial factor in pushing the product up Amazon’s rankings and help gain algorithmically calculated endorsements, such as the influential “Amazon’s Choice” badge.

“You are more than twice as likely to choose an inferior product online versus the best product online if there are fake reviews on those inferior products,” said Neena Bhati, head of campaigns at consumer group Which?. The organization has campaigned heavily for more stringent checks on online reviews.

© 2020 The Financial Times Ltd. All rights reserved Not to be redistributed, copied, or modified in any way.

https://arstechnica.com/?p=1703675