ProtonMail founder: Apple uses monopoly to “hold all of us hostage”

reader comments

73 with 44 posters participating, including story author

Share this story

The developer behind secure email service ProtonMail today came out swinging against the way Apple allegedly uses its App Store to control access to iOS users and cut out competitors. The company is all but begging regulators to take stronger action.

“Apple has become a monopoly, crushing potential competitors with exploitative fees and conducting censorship on behalf of dictators,” ProtonMail founder and CEO Andy Yen wrote in a company blog post. “We know this because we have quietly tolerated this exploitation for years.”

Apple, Yen claimed, is using its market power “to hold all of us [developers] hostage.” Referring to the 30 percent cut Apple takes of any sales through its App Store as a “tax,” he added that traditional analogies to retail space break down when it comes to software:

> *Apple attempts to justify these fees by arguing that the App Store is no different from a mall, where companies seeking to offer their products must pay rent to the owner of the mall (in this case, Apple). This argument conveniently ignores the fact that there is just a single mall when it comes to iOS*

> *and no possibility of a competing mall to rent space from. It is not illegal for Apple to own a mall and rent space, nor is it illegal for Apple to own the only mall. What is illegal, is exploiting the fact that it owns the only mall to charge excessively high pricing which harms competitors.*

"This is virtually indistinguishable from a protection racket," Yen argued. "It is a fee that developers must pay if they want to stay in business. And it is a fee which ultimately harms consumers because these fees are indirectly passed on to users, either through higher prices or through fewer competing products in the marketplace."

ProtonMail is not the first to argue that Apple's 30 percent cut amounts to a tax that cuts unfairly into other firms' revenue and makes it harder to compete against Apple's first-party apps. This behavior is not only illegal, Yen wrote, but "leveraging this power to suppress digital freedom is simply unethical, and it is long overdue that somebody called out Apple for this behavior."

Widespread claims

Amazon, Facebook, and Google tend to be in the hot seat more often when it comes to matters of trustbusting, anticompetitive behavior, and potential abuse of market power. But Apple, too, is facing a bevy of probes—not only in the United States, but especially in Europe.

Spotify filed an antitrust complaint against Apple with European regulators in March 2019. "Apple has introduced rules to the App Store that purposely limit choice and stifle innovation at the expense of the user experience," company founder and CEO Daniel Ek said at the time. Ereader service Kobo joined the complaint in June of this year.

The European Commission's preliminary investigation found

“concerns that Apple’s restrictions may distort competition for music streaming services on Apple’s devices,” and last month the EU formally opened a deeper probe into Apple’s App Store and its Apple Pay payment system.

David Heinemeier Hansson, founder of email-management service Hey, publicly complained last month that Apple privileged its own services over third-party apps such as his. “You listen to some of these app developers, and they sound like hostages,” Hansson told Protocol. “They sound like they’re reading a prepared statement, because otherwise Apple could hurt their business. Which is true!”

Messaging app Telegram also joined the fray last week, when it, too filed a complaint with the EU alleging Apple was abusing its “monopolistic power” to stifle innovation.

https://arstechnica.com/?p=1696045

Ajit Pai calls for “vigorous debate” on Trump’s social media crackdown

Enlarge / FCC Chairman Ajit Pai.

reader comments

40 with 33 posters participating

Share this story

The Federal Communications Commission today asked the public for responses to the Trump administration's attempt to punish social media websites for alleged anti-conservative bias.

"Longstanding rules require the agency to put such petitions out for public comment 'promptly,' and we will follow that requirement here," FCC Chairman Ajit Pai said.

Trump issued an executive order in May, instructing the National Telecommunications and Information Administration (NTIA) to petition the FCC for a new interpretation of Section 230 of the Communications Decency Act that would limit social media platforms' legal protections for hosting third-party content when the platforms take down content they consider objectionable.

The NTIA filed that petition last week, asking the FCC to define "information content provider" more broadly to include entities that make "editorial decisions that modify or alter content." Under that interpretation, websites like Facebook and Twitter would be treated as the publisher or speaker of information posted by their users, and they would lose the legal protections Section 230 provides when websites block and screen offensive material. Lawyers who work at several advocacy groups say that the FCC doesn't have this authority, that the Trump petition "is utterly incompatible with the plain language" of Section 230, and that the petition's proposal would violate the First Amendment.

The FCC's public notice asking for comments says that "Interested persons may file statements opposing or supporting the Petition for Rulemaking." The deadline for initial statements is 30 days from today, and another 15 days will be provided for replies. The docket is available here (click "New Filing" or "Express" to file a comment).

The FCC's call for comments takes no position on whether the

Trump administration petition should be approved. If the FCC were close to issuing new rules, it would likely release a Notice of Proposed Rulemaking that makes a specific proposal and asks the public a series of questions. But right now, the FCC is just asking the public to weigh in on whether the NTIA petition should be granted.

Pai's statement said the FCC should "welcome vigorous debate," but he didn't commit to taking any further action in response to the Trump administration petition. Pai said:

> *I strongly disagree with those who demand that we ignore the law and deny the public and all stakeholders the opportunity to weigh in on this important issue. We should welcome vigorous debate—not foreclose it. The American people deserve to have a say, and we will give them that chance. Their feedback over the next 45 days will help us as we carefully review this petition."*

"Tell the FCC to reject this"

The FCC's two Democrats continued their opposition to the petition today. "Social media can be frustrating. But the FCC shouldn't be the President's speech police," FCC Commissioner Jessica Rosenworcel wrote on Twitter. "So speak up. Tell the FCC to reject this loud and clear."

FCC Commissioner Geoffrey Starks weighed in on Twitter, too, writing, "I'm sure this Public Notice will generate a spirited discussion. Perhaps when comments are in we can package up the whole docket and send it over to Congress—where this debate belongs."

Starks previously said that the NTIA petition "has not made the case that Congress gave the FCC any role here. Section 230 is best understood as it has long been understood: as an instruction to courts about when liability should not be

imposed."

FCC Republican Brendan Carr enthusiastically praised Trump's proposal shortly after the executive order came out in May. But FCC Republican Michael O'Rielly has expressed "deep reservations" about the Trump order.

In a speech last week, O'Rielly said, "The First Amendment protects us from limits on speech imposed by the government—not private actors—and we should all reject demands, in the name of the First Amendment, for private actors to curate or publish speech in a certain way. Like it or not, the First Amendment's protections apply to corporate entities, especially when they engage in editorial decision making."

Although O'Rielly's statement would seem to reject the position taken in Trump's executive order, O'Rielly clarified that his "critique is not in any way directed toward President Trump or those in the White House." Trump and his administration "are fully within their rights to call for the review of any federal statute's application, the result of which would be subject to applicable statutory and constitutional guardrails," O'Rielly said.

https://arstechnica.com/?p=1696078

Trump administration gives TikTok 45 days to sell to

Microsoft or leave US [Updated]

Enlarge / TikTok’s US operations may soon be part of every cool teen’s favorite code conglomerate, Microsoft.

reader comments

353 with 173 posters participating

Share this story

After weeks of rumor and speculation, the Trump administration this weekend gave TikTok’s parent company, Beijing-based ByteDance, 45 days to sell off the social media sensation or else stop operating in the United States—and Microsoft looks to be the buyer.

Microsoft on Sunday confirmed what several media outlets had been speculating since Friday, saying it is in talks to buy TikTok’s operations in the US, Canada, Australia, and New Zealand and may also invite other US investors to take minority stakes in the deal.

“Microsoft will move quickly to pursue discussions with TikTok’s parent company, ByteDance, in a matter of weeks, and in any event completing these discussions no later than September 15, 2020,” the company said in a corporate blog post. “During this process, Microsoft looks forward to continuing dialogue with the United States Government, including with the President.”

Specifically, the transaction would take place to allay US concerns about data being stored in China and possibly accessed by the Chinese government, the blog post said:

> *This new structure would build on the experience TikTok users currently love, while adding world-class security, privacy, and digital safety protections. The operating model for the service would be built to ensure transparency to users as well as appropriate security oversight by governments in these countries.*
>
> *Among other measures, Microsoft would ensure that all private data of TikTok's American users is transferred to and remains in the United States. To the extent that any such data is currently stored or backed-up outside the United States, Microsoft would ensure that this data is deleted from servers outside the country after it is transferred.*

A national security threat?

US regulators have been expressing concerns about TikTok's Chinese ownership since last year. In October, Senate leaders from both parties pushed for intelligence agencies to open an investigation of TikTok. "TikTok's terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information," the senators wrote at the time. "While the company has stated that TikTok does not operate in China and stores US user data in the US, ByteDance is still required to adhere to the laws of China."

By the time a week had passed, regulators were obliging—the Committee on Foreign Investment in the United States, or CFIUS, opened a review in November. CFIUS, which is based in the Treasury Department, comprises members from several agencies that review transactions in which a foreign buyer acquires a US firm for potential national security concerns. Since 2019, CFIUS has expanded authority also to investigate certain kinds of major investments that aren't straight

acquisitions as well.

TikTok was formed when ByteDance bought US firm Musical.ly for roughly $1 billion in 2017 and then rebranded and relaunched it under the TikTok name. CFIUS did not review the Musical.ly deal at the time, but it has the authority to do so retroactively—as it now is. That kind of review is what led to President Donald Trump's 2018 executive order prohibiting Broadcom from purchasing rival Qualcomm (even though Qualcomm had vehemently turned down every single offer Broadcom made it).

Secretary of State Mike Pompeo said in July that the administration was considering an outright ban on TikTok as well as potentially expanding that type of ban to other Chinese firms. "With respect to the Chinese apps on people's cell phones I can assure you the United States will get this one right," Pompeo said. "I don't want to get out in front of the president, but it's something we're looking at."

Tick… tock…

Trump on Friday night said unequivocally that he wanted to ban TikTok. "As far as TikTok is concerned, we're banning them from the United States. … I have that authority," he told reporters while on Air Force One, indicating an executive order could come as soon as Saturday.

Other officials inside the administration, including Treasury Secretary Steven Mnuchin, pushed for a sale instead of a ban, sources told Reuters and the Wall Street Journal. Microsoft CEO Satya Nadella spoke by phone with Trump on Sunday, after which the White House agreed to the 45-day sale deadline and Microsoft made its public statement about the potential deal.

Update 3:23pm ET: In the hours after Ars published this story, President Trump told reporters he approved of the potential Microsoft transaction.

If Nadella wants to “go ahead” with the deal, “he can try,” Trump said. “We set a date, I set a date, of around September 15th, at which point it’s going to be out of business in the United States. But if somebody, whether it’s Microsoft or somebody else, buys it, that’ll be interesting.”

Inexplicably, Trump also added: “More than anything else, I said a very substantial portion of that price is going to have to come into the Treasury of the United States. Because we’re making it possible for this deal to happen. Right now, they don’t have any rights, unless we give it to them. So if we’re going to give them the rights, then it has to come into, it has to come into this country.”

The commission he imagines the federal government receiving from the deal seemed to be foremost on his mind. “So it’ll close down on September 15th, unless Microsoft or somebody else is able to buy it, and work out a deal, an appropriate deal, so the Treasury of the— really the Treasury, I suppose you would say, of the United States, gets a lot of money. A lot of money,” Trump concluded.

Although the administration can arguably require ByteDance to divest TikTok on national security grounds, Trump did not explain what legal basis or mechanism would make his proposal that the United States get a cut—a “lot of money” or otherwise—from the transaction possible.

https://arstechnica.com/?p=1695888

SpaceX now plans for 5

million Starlink customers in US, up from 1 million

Enlarge / A SpaceX Starlink user terminal/satellite dish.

reader comments

126 with 87 posters participating

Share this story

SpaceX has asked the US for permission to deploy up to 5 million user terminals for its Starlink satellite-broadband network in the US after nearly 700,000 people in the country registered interest in the service.

SpaceX in March received a Federal Communications Commission license for up to 1 million user terminals (i.e. satellite dishes) in the United States. That would allow for 1 million homes to receive the service, but SpaceX now wants to quintuple that number.

“SpaceX Services requests this increase in authorized units due to the extraordinary demand for access to the Starlink non-geostationary orbit satellite system,” the company told the FCC in a license-change request on Friday. “Despite the fact that SpaceX has yet to formally advertise this system’s services, nearly 700,000 individuals represented in all 50 states signed up over a matter of just days to register their interest in said services at www.starlink.com. To ensure that SpaceX is able to accommodate the apparent demand for its broadband Internet access service, SpaceX Services requests a substantial increase in the number of authorized units.”

SpaceX added the signup form to the Starlink website in mid-

June. It asks people to enter their email and street address to “get updates on Starlink news and service availability in your area.” SpaceX has said it will offer beta access in the fall of this year to prepare for a full commercial launch.

The 700,000 people who registered interest haven’t committed to purchasing anything, but Starlink will likely have many potential buyers in the US among people who either lack fiber or cable Internet access or are stuck with a single provider and no other choices.

Starlink mostly targeted at rural homes

Starlink will face some physical limits on how many homes it can serve in densely populated areas such as Los Angeles, SpaceX CEO Elon Musk said recently. “We’ll have some small number of customers in LA. But we can’t do a lot of customers in LA because the bandwidth per cell is simply not high enough,” he said. Starlink wouldn’t face such restrictions in rural areas, as Musk said that “Starlink will serve the hardest-to-serve customers that telcos otherwise have trouble doing with landlines or even with… cell towers.”

SpaceX has FCC permission to launch nearly 12,000 satellites in low-Earth orbits that will allow for much lower latencies than traditional satellite services. SpaceX has launched 540 Starlink satellites so far, with its next launch set to increase that number to about 600.

Amazon last week received US approval to launch 3,236 low-Earth orbit satellites for its similar “Project Kuiper” broadband service.

https://arstechnica.com/?p=1695911

What’s this? A bipartisan plan for AI and national security

Enlarge / Closeup of a Predator MQ-9 uncrewed aerial vehicle.

reader comments

30 with 15 posters participating

Share this story

US Reps. Will Hurd and Robin Kelly are from opposite sides of the ever-widening aisle, but they share a concern that the United States may lose its grip on artificial intelligence, threatening the American economy and the balance of world power.

On Thursday, Hurd (R-Tex.) and Kelly (D-Ill.) offered suggestions to prevent the US from falling behind China, especially, on applications of AI to defense and national security. They want to cut off China’s access to AI-specific silicon chips and push Congress and federal agencies to devote more resources to advancing and safely deploying AI technology.

Although Capitol Hill is increasingly divided, the bipartisan duo claims to see an emerging consensus that China poses a serious threat and that supporting US tech development is a vital remedy.

“American leadership and advanced technology has been critical to our success since World War II, and we are in a race with the government of China,” Hurd says. “It’s time for Congress to play its role.”

Kelly, a member of the Congressional Black Caucus, says that she has found many Republicans, not just Hurd, the only Black Republican in the House, open to working together on tech issues. “I think people in Congress now understand that we need to do more than we have been doing,” she says.

The Pentagon’s National Defense Strategy, updated in 2018, says AI will be key to staying ahead of rivals such as China and Russia. Thursday’s report lays out recommendations on how Congress and the Pentagon should support and direct use of the technology in areas such as autonomous military vehicles. It was written in collaboration with the Bipartisan Policy Center and Georgetown’s Center for Security and Emerging Technology, which consulted experts from government, industry, and academia.

The report says the US should work more closely with allies on AI development and standards, while restricting exports to China of technology such as new computer chips to power machine learning. Such hardware has enabled many recent advances by leading corporate labs, such as at Google. The report also urges federal agencies to hand out more money and computing power to support AI development across government, industry, and academia. The Pentagon is asked to think about how court martials will handle questions of liability when autonomous systems are used in war and to talk more about its commitment to ethical uses of AI.

Hurd and Kelly say military AI is so potentially powerful that America should engage in a kind of AI diplomacy to prevent

dangerous misunderstandings. One of the report's 25 recommendations is that the US establish AI-specific communication procedures with China and Russia to allow human-to-human dialog to defuse any accidental escalation caused by algorithms. The suggestion has echoes of the Moscow-Washington hotline installed in 1963 during the Cold War. "Imagine in a high-stakes issue: What does a Cuban missile crisis look like with the use of AI?" asks Hurd, who is retiring from Congress at the end of the year.

Cut through the hype

Beyond such worst-case scenarios, the report includes more sober ideas that could help dismantle some hype around military AI and killer robots. It urges the Pentagon to do more to test the robustness of technologies such as machine learning, which can fail in unpredictable ways in fast-changing situations such as a battlefield. Intelligence agencies and the military should focus AI deployment on back-office and noncritical uses until reliability improves, the report says. That could presage fat new contracts to leading computing companies such as Amazon, Microsoft, and Google.

Helen Toner, director of strategy at the Georgetown center, says although the Pentagon and intelligence community are trying to build AI systems that are reliable and responsible, "there's a question of whether they will have the ability or institutional support." Congressional funding and oversight would help them get it right, she says.

The paper released Thursday is the second of four on AI strategy issued by Hurd and Kelly with the Bipartisan Policy Center. The first, released earlier this month, focused on the workplace. Its recommendations included reworking education from kindergarten through grad school to prepare more Americans to work with or on AI. The two papers to come are on AI research and development, and AI ethics.

Kelly and Hurd have shared an interest in AI since working on hearings on the subject by the House Oversight Committee's Subcommittee on Information Technology in 2018. The pair later authored a report warning that the US could lose its leading position on AI. Kelly says she wants to ensure the United States remains a leader in AI, but also that "people in the diverse district I come from have a piece of that pie, and that there are not biases against them or concerns around privacy."

Falling behind

At the tail end of the Obama administration, the White House produced lengthy documents on how to support US AI development and deployment and address potential downsides such as technological unemployment. The Trump administration chose not to build on those, but last year President Trump signed an executive order directing existing government programs to be tilted towards AI projects. It leaves the US with a less toothy AI strategy than many other nations, including China, which have stood up new programs and funding sources. Hurd and Kelly are trying to change that.

James Lewis, who leads work on technology policy at the Center for Strategic and International Studies, applauds the effort. The timing is good, he says, because more lawmakers are taking an interest in tech policy. "They now realize we're in a contest with China and have woken up to the fact that technology like AI and semiconductors and cybersecurity are important," he says. Last week, the Senate voted 96-4 to amend the annual Pentagon budget bill with $25 billion to support domestic research and manufacturing of new chip technology.

Lewis supports restricting chip exports to China—an idea that could gain traction in a Congress showing new interest in tech export controls. He's skeptical that an AI hotline or inventing special forms of AI diplomacy to prevent autonomous

accidents are worthwhile. Events during the Cold War and since, most recently in areas such as cybersecurity, suggest China and Russia don’t take such programs seriously, Lewis says.

Hurd and Kelly are now drafting a congressional resolution incorporating their ideas about AI, including in national security. After that, they’ll start work on AI legislation. “Some of that I hope we get done in this Congress, and others can be taken and run with in the next Congress,” Hurd says.

This story first appeared on wired.com.

https://arstechnica.com/?p=1695629

Florida teen charged as “mastermind” in Twitter hack hitting Biden, Bezos, and others

reader comments

148 with 116 posters participating

Share this story

Authorities on Friday charged three people with orchestrating this month’s epic hack of Twitter and using it to generate

more than $100,000 in a bitcoin scam promoted by hijacked accounts of politicians, executives, and celebrities.

Federal prosecutors in San Francisco charged Mason Sheppard, 19, Nima Fazeli, 22, and an unnamed juvenile in the July 15 breach. Prosecutors in Florida, where the juvenile defendant lives, identified him as 17-year-old Graham Ivan Clark and charged him with 30 felony charges. Federal prosecutors said that Sheppard used the hacking names “Chaewon” and “ever so anxious#001” and resides in the UK town of Bognor Regis. Fazeli, who allegedly called himself “Rolex,” “Rolex#0373,” “Rolex#373,” and “Nim F,” is from Orlando, Florida.

The three suspects stand accused of using social engineering and other techniques to gain access to internal Twitter systems. They then allegedly used their control to take over what Twitter has said were 130 accounts. A small sampling of the account holders included former Vice President Joe Biden, Tesla founder Elon Musk, pop star Kanye West, and philanthropist and Microsoft founder, former CEO, and Chairman Bill Gates.

The defendants, prosecutors alleged, then caused the high-profile accounts—many of them with millions of followers—to promote scams that promised to double the returns if people deposited bitcoins into attacker-controlled wallets. The scheme generated more than $117,000. The hackers also took over accounts with short user names, which are highly coveted in a criminal hacking forum circle calling itself OGusers.

“These crimes were perpetrated using the names of famous people and celebrities, but they’re not the primary victims here,” said Hillsborough State Attorney Andrew Warren. “This ‘Bit-Con’ was designed to steal money from regular Americans from all over the country, including here in Florida. This massive fraud was orchestrated right here in our backyard, and we will not stand for that.”

Painstaking recon, social engineering, and carefully timed phishing

A security researcher who has been actively working with the FBI on the investigation into this month's breach told Ars that the hack was the result of painstaking research into Twitter employees, the social engineering of them by phone, and carefully timed phishing.

Allison Nixon, chief research officer at security firm Unit 221B, said evidence collected to date shows that Clark and hackers he worked with started by scraping LinkedIn in search of Twitter employees who were likely to have access to the account tools. Using features that LinkedIn makes available to job recruiters, the attackers then obtained those employees' cell phone numbers and other private contact information.

The attackers then called the employees and used the information obtained from LinkedIn and other public sources to convince them they were authorized Twitter personnel. Work-at-home arrangements caused by the COVID-19 pandemic also prevented the employees from using normal procedures such as face-to-face contact to verify the identities of the callers.

With the confidence of the targeted employees, the attackers directed them to a phishing page that mimicked an internal Twitter VPN. The attackers then obtained credentials as the targeted employees entered them. To bypass two-factor authentication protections Twitter has in place, the attackers entered the credentials into the real Twitter VPN portal within seconds of the employees entering their info into the fake one. Once the employee entered the one-time password, the attackers were in.

Nixon and Unit 221B chief legal officer Mark Rasch laid out a description of the hackers' tactics, techniques, and

procedures in a post published shortly after the charges were filed.

ID’d through a hacked database

Prosecutors said they tracked Sheppard and Fazeli through an OGusers forum database that was stolen and published by a group of rival hackers. The database—which the FBI obtained in early April, more than three months before the Twitter hack—contained public forum postings, private messages, IP addresses, email addresses, and other user information of forum participants.

On the day of the Twitter breach, someone with the OGusers account name “Chaewon” advertised that he could change email addresses associated with any Twitter account for $250 and would give direct access to accounts for for $2,500 to $3,000. Chaewon referred buyers to contact the Discourt user ever so anxious#0001.

The OGusers database showed that in early February, a user with the name Chaewon offered to buy a compromised video game account. FBI investigators found that the wallet address that made the payment belonged to the same Bitcoin cluster that ever so anxious#001 used on July 15 to received payments before sending them to an address belonging to Kirk#5270. A Bitcoin cluster is a group of wallets that can be forensically tied to a single individual or entity.

Investigators also used IP addresses Chaewon used to connect to OGusers to tie him to a different OGuser account with the name “Mas,” which was associated with the email address masonshppy@gmail.com. Records investigators got from the Coinbase currency exchange showed that the address was associated with an account owned by a Matthew Sheppard. A drivers license provided by the user of the Coinbase account belonged to Sheppard.

Investigators identified Fazeli when the hacked OGuser database showed someone with the username “Rolex” proving he had control of a Discord account that was registered to a “Rolex#0373.” In Discord chats that occurred on the day of the Twitter breach, Rolex#0373 had acted as a broker for accounts another alleged hacking participant, with the Discord username Kirk#5270, was advertising for sale.

On OGusers, Rolex also used the email address chancelittle10@gmail.com on multiple occasions in 2018 to receive PayPal payments from other users. The same discussion on Discord showed Rolex#0373 paying Kirk#5270 $500 for control of the hijacked Twitter account @foreign. Rolex#0373 instructed the address associated with the Twitter account be changed to chancelittle10@gmail.com.

“Charged as adults”

Sheppard is charged with one count each of aiding and abetting intentional access of a protected computer and obtaining information, conspiracy to commit wire fraud, and conspiracy to commit wire fraud. Fazeli is charged with a single count of computer intrusion. Hillsborough County prosecutors, who called Clark the mastermind of the breach, charged him with one count of organized fraud, 11 total counts of fraudulent use of personal information, one count of accessing a computer or electronic device without authority, and 17 counts of communications fraud.

Clark’s prosecution is taking place in Tampa, where he lives, “because Florida law allows minors to be charged as adults in financial fraud cases such as this when appropriate,” Warren’s office said.

https://arstechnica.com/?p=1695665

Amazon investing $10 billion to compete against SpaceX in satellite broadband

Getty Images | Yuichiro Chino

reader comments

242 with 105 posters participating

Share this story

Amazon has received US approval to launch 3,236 low-Earth orbit satellites for its planned “Project Kuiper” broadband service.

A Federal Communications Commission order granting Amazon’s application was released Thursday. Amazon said in a blog post that it will invest more than $10 billion in the project.

“This investment will create jobs and infrastructure around the United States, build and scale our ground network, accelerate satellite testing and manufacturing, and let us deliver an affordable customer terminal that will make fast, reliable broadband accessible to communities around the world,” Amazon said. Amazon will target areas without good Internet service and said that “Project Kuiper will deliver high-speed, low-latency broadband service to places beyond the reach of traditional fiber or wireless networks.”

The planned satellites would orbit at altitudes of 590km,

610km, and 630km, allowing latencies far lower than traditional satellite services that use geosynchronous orbits of more than 35,000km. That's similar to SpaceX's Starlink, but SpaceX is much further along, as it has launched about 600 satellites and is getting ready to start beta trials with customers.

Service to begin once 578 satellites launch

FCC rules give Amazon six years to launch and operate 50 percent of the licensed satellites, with a deadline date of July 30, 2026. Amazon would have to launch the rest of the licensed satellites by July 30, 2029.

Amazon plans to offer broadband to customers "once the first 578 satellites are launched," the FCC said. Amazon hasn't said when service will be available to customers.

The FCC approval said Amazon's plan would "provid[e] continuous coverage to customers within approximately 56°N and 56°S latitude, thereby serving the contiguous United States, Hawaii, US territories, and other world regions." The plan calls for using frequencies of 17.7-18.6 GHz and 18.8-20.2 GHz for space-to-Earth communications, and 27.5-30.0 GHz for Earth-to-space transmissions. The FCC said it granted the license because it "would advance the public interest by authorizing a system designed to increase the availability of high-speed broadband service to consumers, government, and businesses."

Amazon filed the FCC application in July 2019—more details on Amazon's plan are available in our story on the application.

The FCC approval includes requirements for minimizing orbital debris and collision risk, prevention of harmful interference, spectrum sharing, and power limits. Amazon's design of the

Kuiper satellites is not complete, so the company will need another FCC approval after it submits a final plan for orbital-debris mitigation, collision risk, and “re-entry casualty risk.” The FCC approval is also conditioned on Amazon getting a “favorable” rating from the International Telecommunication Union to show compliance with power limits.

Besides SpaceX, Amazon’s Project Kuiper would potentially face low-Earth satellite competition from OneWeb, which filed for bankruptcy in late March. On July 3, OneWeb agreed to sell the business to a consortium including the UK government and Bharti Global Limited. The UK government, which is investing $500 million, said, “The deal will enable the company to complete construction of a global satellite constellation that will provide enhanced broadband and other services to countries around the world.” OneWeb also has an investment from Hughes, which operates geosynchronous satellites.

https://arstechnica.com/?p=1695558

“This is a very dangerous situation”: Big Tech’s day on the Hill

Enlarge / Amazon CEO Jeff Bezos testifies (remotely) before the House Judiciary Subcommittee on Antitrust, Commercial and Administrative Law hearing on “Online Platforms and Market Power” in the Rayburn House Office Building on Capitol Hill in Washington, DC on July 29, 2020.

reader comments

98 with 71 posters participating, including story author

Share this story

A bevy of tech's biggest titans—Alphabet CEO Sundar Pichai, Amazon CEO Jeff Bezos, Apple CEO Tim Cook, and Facebook CEO Mark Zuckerberg—all took to their remote offices Wednesday to dial into a hotly anticipated Congressional hearing, the latest part of an in-depth investigation into their firms' behavior that began more than a year ago.

The almost six-hour hearing was nominally convened to talk about antitrust enforcement, and it had two core questions at its heart. First: do the biggest, globe-spanning US tech companies have too much power in the market? And second: did they come by the power they do have honestly, or did they somehow cheat to get it?

House Antitrust Subcommittee Chairman Rep. David Cicilline (D-R.I.) focused his opening remarks on how bipartisan the investigation process has been to date before sketching out his belief that all four companies present have behaved anticompetitively, become monopolies, and caused harm both to consumers and the entire democratic project writ large.

"When everyday Americans learn how much of their data is being mined, they can't run away fast enough," Cicilline said. "But in many cases, there is no escape from the surveillance, because there is no alternative. People are stuck with bad options.

"As gatekeepers of the digital economy, these platforms enjoy the power to determine winners and losers, to shake down small businesses and enrich themselves while choking off competitors," said Cicilline. "Their ability to dictate terms, call the shots, upend entire sectors, and inspire fear represents the powers of a private government. Our founders

would not bow before a king, nor should we bow before the emperors of the online economy."

"Being big is not inherently bad," Ranking Member Jim Sensenbrenner (R-Wis.) added in his opening remarks, but the platforms can still have deleterious effects on the marketplace. "My colleagues and I have a great interest in what your companies do with [their] accumulated power.

"Conservatives are consumers, too, and they need the protection of the antitrust laws," Sensenbrenner said, hinting at the argument most of his Republican colleagues would later make. "The power to influence debate carries with it remarkable responsibilities, so let the facts be our guide here. Your companies are large; that's not a problem. Your companies are successful; that's not a problem, either. But I want to leave here with a more complete picture of how your companies use their size, success, and power and what it means to the American consumer."

All four CEOs in their opening statements (Apple, Amazon, Facebook, Google) strived to position themselves as plucky American success stories, job creators, drivers of economic success, and necessary alternatives to China, but they also argued their companies face intense competition on all sides.

Both the lawmakers and the witnesses stayed roughly on topic to begin with. But once the question-time portion of the festivities began, suddenly everyone had a pet issue to dig into. Democrats by and large tended to focus on issues related to competition, while Republicans zeroed in on alleged bias, leading the proceeding to feel almost like two overlapping hearings struggling to occupy the same moment in space-time.

On gatekeeping

Last year, as the antitrust investigation ramped up, the subcommittee requested decades' worth of internal documents

from all four companies. Damning passages from those documents took center stage as the lawmakers challenged the CEOs about competition—and the lawmakers brought receipts.

During questioning, members of the committee zeroed in on the ways the four companies have been accused of stifling other businesses in the space. “Over 85 percent of all online searches go through Google,” Cicilline said to Pichai, as soon as questioning started. “Numerous businesses told us that Google steals their content and privileges its own sites in ways that profit Google but crush everyone else… Did Google ever use its surveillance over Web traffic to identify competitive threats?”

Pichai tried to dodge the question, responding, “Just like other businesses, we try to understand trends from data, which we can see, and we use it to improve our products for users.”

Later, House Judiciary Committee Chairman Jerrold Nadler (D-N.Y.) returned to press the issue harder, to which Pichai again hedged, “Just like other businesses, we try to understand trends from, you know, data, which we can see, and we use it to improve our products for users.”

“What’s to stop Apple?”

Apple, too, faced accusations that it could leverage its data against potential competition.

Rep. Hank Johnson (D-Ga.) took Cook to task over the walled garden of the App Store and challenged Apple’s ability to play gatekeeper and gather app distribution data even though its own first-party apps compete against third-party App Store offerings.

“With over 100 million iPhone users in the United States alone, and with Apple’s ownership of the App Store giving Apple the ability to control which apps are allowed to be

marketed to Apple users, you hold immense power over small businesses to grow and prosper," Johnson said. The rules of the store can be opaque and are "arbitrarily enforced," he went on, and iOS app developers have no choice but to roll with it. "Does Apple not treat all app developers equally?"

"We treat every developer the same," Cook replied. "We have open and transparent rules."

The committee, however, obtained emails showing that Apple agreed to halve its fee for revenue generated through Amazon's apps. Apple likewise waives its cut for certain streaming video services in exchange for those developers agreeing to integrate certain Apple features into their apps.

"What's to stop Apple from increasing its commission to 50 percent?" Johnson asked.

"We have never increased commissions in the store since the first day it operated," Cook responded, denying that there was no mechanism for preventing it. "There is a competition for developers just as there is a competition for customers. They could develop their app for Android or Windows or Xbox or Playstation… so competitive I would describe it as a street fight for market share in the smartphone business."

Several members pressed Amazon about its use of data generated by third-party merchants who use its marketplace as a selling platform.

"You've referred to third-party sellers today as Amazon's 'partners' and said that your success depends on their success," Rep. Lucy McBath (D-Ga.) said to Bezos. "But over the past year, we've heard a completely different story."

Small-business owners that spoke with the committee members described their relationship with Amazon using words such as "bullying," "fear," and "panic," McBath went on, before she played back a recording of a bookseller whose Amazon

marketplace business was allegedly delisted in 2019 in retaliation for becoming too large.

Rep. Pramila Jayapal (D-Wash.) echoed the charge. “You have access to data that your competitors do not have, so you might allow third-party sellers onto your platform,” she explained to Bezos. “But if you are continuously monitoring the data to make sure that they’re never going to get big enough that they can compete with you, that is actually the concern that the committee has.”

Jayapal concluded:

> *The whole goal of this committee’s work is to make sure that there are more Amazons, that there are more Apples, that there are more companies that get to innovate and small businesses that get to thrive, and that is what we’re trying to get at—that is why we need to regulate these marketplaces—so that no company has a platform so dominant that it is essentially a monopoly.*

https://arstechnica.com/?p=1694916

Emails detail Amazon’s plan to crush a startup rival with price cuts

Enlarge / Jeff Bezos speaks via videoconference during a House Judiciary Committee meeting on Wednesday, July 29, 2020.

reader comments

181 with 121 posters participating, including story author

Share this story

Emails published by the House Judiciary Committee this week confirm an accusation that critics have long leveled against Amazon: that the company's aggressive price-cutting for diapers in 2009 and 2010 was designed to undercut an emerging rival.

That rival, Quidsi, had gained traction with a site called Diapers.com that sold baby supplies. Amazon had good reason to worry. As journalist Brad Stone wrote in his 2013 book about Amazon, Bezos' company didn't start selling diapers until a year after Diapers.com did. At the time, diapers were seen as too bulky and low-margin to be delivered profitably.

But Quidsi's founders figured out how to do it. They optimized their packaging for baby products and positioned warehouses close to metropolitan areas. That not only allowed them to get cheaper ground-shipping rates—it also allowed them to provide overnight shipping to most of their customers—in many cases, faster than Amazon's own shipping.

Quidsi's plan was to gradually expand into other retail categories, much as Amazon had done a decade earlier. If Quidsi's growth had continued unchecked, the company could have become a major Amazon rival. But Amazon made sure that didn't happen—first by launching a brutal price war, then by buying the company. The new emails provide an inside view into Amazon's thinking during this fight.

At Wednesday's hearing before the House Judiciary Committee, Rep. Mary Gay Scanlon (D-Pa.) confronted Bezos about Amazon's aggressive diaper price-cutting. Bezos responded he didn't remember the specifics.

“What I can tell you is that the idea of using diapers and products like that to attract new customers who have new families is a very traditional idea,” Bezos said.

When Scanlon asked how families benefitted from Amazon raising prices after driving out a major competitor, Bezos responded, “I don’t agree with that premise.” He noted that there were many other places to buy diapers, including numerous brick-and-mortar retailers.

“They are our biggest competitor in the diaper space”

By early 2009, Quidsi’s growth had attracted the attention of Amazon executives. “They are our biggest competitor in the diaper space,” wrote Amazon executive Doug Herrington in an email obtained by the House Judiciary Committee. “They keep the pressure on pricing on us. They apparently have lower fulfillment costs than we have.”

In a followup a few minutes later, he wrote that “we need to match pricing on these guys no matter the cost.”

According to Stone, an Amazon executive met with Quidsi’s founders in 2009 and encouraged them to consider selling the company. The founders declined. Soon afterward, Amazon slashed its diaper prices by as much as 30 percent.

But Quidsi kept growing. By 2010, the company had earned the loyalty of thousands of young parents and had reached $300 million in revenue.

In June 2010, Quidsi announced it was expanding to a second product category with a new site, soap.com. That got the attention of Jeff Bezos, who asked several subordinates for their thoughts in a June 8 email.

“Given diapers.com’s strength and competencies, soap.com is

our most significant short-term competitor in the hpc space," Herrington replied to Bezos and other Amazon execs (HPC is apparently a reference to "health and personal care"—one of Amazon's product categories).

"We have already initiated a more aggressive 'plan to win' against diapers.com in the diaper/baby space," Herrington continued. In addition to offering "market leading pricing on diapers," Herrington wrote, Amazon was preparing to launch a new "Amazon Mom" program that offered parents deeper discounts on diapers and related products if customers signed up for a subscription.

Amazon ratchets up the pressure

Quidsi's founders didn't want to sell their company, but Amazon's diaper price war was starting to hurt Quidsi. Growth was slowing, and Quidsi was having trouble raising additional capital to continue expanding.

On September 14, the founders of Quidsi flew to Seattle to meet with Amazon and discuss a possible acquisition. As Quidsi's founders were sitting in a meeting with Amazon brass, Amazon hit Quidsi in the gut. It announced a new program called "Amazon Mom" that offered free Prime service and an additional 30-percent discount on diapers if users signed up to get them through Amazon's monthly "subscribe and save" program. This was a larger discount than Amazon offered on most other Subscribe and Save items.

This put Quidsi in an untenable situation, as Stone writes:

> *That month, Diapers.com listed a case of Pampers at $45; Amazon priced it at $39, and Amazon Mom customers with Subscribe and Save could get a case for less than $30. At one point, Quidsi executives took what they knew about shipping rates, factored in Proctor and Gamble's wholesale prices, and calculated that Amazon was on track to lose $100 million over*

three months in the diapers category alone.

Amazon's losses may have actually been even larger. During Wednesday's hearing, Scanlon said that internal documents obtained by the committee showed Amazon losing $200 million in a single month from diaper products.

Amazon knew it was bleeding Quidsi dry. An internal email later in September discussed the price cuts Quidsi was forced to make to compete with the new Amazon Mom discounts. "They expect to lose lots of money in the next few yrs," wrote executive Peter Krawiec. "This will make it worse."

Quidsi didn't have the money to fight a lengthy price war with Amazon, and venture capitalists were reluctant to give Quidsi more cash to fight what looked like a hopeless battle. So in November, Quidsi reluctantly signed a merger agreement with Amazon.

"I don't remember that"

When Stone was writing his book, an Amazon executive told him that (in Stone's words) "everything Amazon subsequently did in the diapers market [after mid-2010] was planned beforehand and unrelated to competing with Quidsi." But the newly released emails contradict that claim. Herrington specifically listed the Amazon Mom rollout as part of Amazon's "aggressive 'plan to win' against diapers.com." Later in the same email, Herrington wrote that "to the extent this plan undercuts the core diapers business for diapers.com, it will slow the adoption of soap.com."

Amazon's claim is also hard to square with the company's actions post-acquisition. Stone notes that "a month after it announced the acquisition of Quidsi, Amazon closed the [Amazon Mom] program to new members." Then a few weeks later, as the Federal Trade Commission was giving the deal unexpectedly

close scrutiny, Amazon re-opened Amazon Mom—but with smaller discounts. In effect, Amazon hiked diaper prices soon after the acquisition.

When Scanlon asked whether Bezos had signed off on raising diaper prices after the acquisition, Bezos pled ignorance.

“I don’t remember that at all,” he said. “We match competitive prices. I believe we followed diapers.com.”

The FTC ultimately approved the deal. Amazon initially let Diapers.com continue as a separate service but shut it down in 2017.

https://arstechnica.com/?p=1695336

Ex-Google engineer Levandowski asks judge not to send him to prison

Enlarge / Anthony Levandowski exits federal court in San Jose, California, on August 27, 2019.
David Paul Morris/Bloomberg via Getty Images

reader comments

4 with 4 posters participating

Share this story

The federal government on Tuesday asked a federal judge to

sentence Anthony Levandowski to 27 months in prison for theft of trade secrets. In March, Levandowski pled guilty to stealing a single confidential document related to Google's self-driving technology on his way out the door to his new startup. That startup was quickly acquired by Uber, triggering a titanic legal battle between the companies that was settled in 2018.

The government initially charged Levandowski with 33 counts of trade secret theft, with each count related to different confidential documents taken by Levandowski. Levandowski agreed to plead guilty to stealing one of the documents if the government dropped the other charges. It's up to Judge William Alsup to decide the appropriate punishment for Levandowski's single admitted act of trade secret theft.

While the government wants to put Levandowski behind bars for more than two years, Levandowski's lawyers are asking the judge not to send Levandowski to jail at all. They argue that a year of home confinement, along with a fine, restitution, and community service, is an adequate punishment. They note that Levandowski has suffered two bouts of pneumonia in recent years, putting him at high risk if he were to catch COVID-19 while in prison.

Dueling portraits in dueling legal briefs

In their Tuesday legal briefs, lawyers for Levandowski and the government paint very different portraits of Levandowski's crime. The government portrays Levandowski as scheming to steal technical specifications of Google's lidar technology so that he could sell them to Uber and use the documents to build competing products. The feds claim that Levandowski was already in acquisition talks with Uber before he'd even officially given Google notice that he was leaving.

“The details about Levandowski’s contacts and negotiations with Uber support the inference that he intended to convert a trade secret to the economic benefit of someone other than the owner thereof,” the government writes.

By contrast, Levandowski’s lawyers deny that he intended to use the documents to aid his new employer—or that he ever did so.

“While it was never in dispute that Mr. Levandowski possessed some Google documents after leaving his job, there is no evidence that Mr. Levandowski used or shared any of Google’s proprietary or trade secret information with employees at Uber or anyone else,” Levandowski’s lawyers write. “Google engaged an army of lawyers and forensic experts to comb through Uber’s facilities, servers, source code, design files, and prototypes—making 12 separate installations in all.”

Federal investigators also looked for evidence of wrongdoing, the lawyers noted. “None of these efforts produced any evidence that Mr. Levandowski used any of Google’s trade secrets after leaving Google’s employment, whether at Uber or anywhere else.”

Levandowski’s lawyers argue that the government has misconstrued the oft-cited statistic that Levandowski downloaded 14,000 documents from a Google server.

The documents were stored using a Subversion source-control system. The Waymo engineer who set up the server testified (in the words of Levandowski’s lawyers) that “in order to review even just a single one of the files, an authorized user such as Mr. Levandowski would have to initiate a checkout command that would automatically download all 14,000 files at one time.” The same Waymo engineer said that “we all do full checkouts, and it makes me uncomfortable that lawyers are trying to ascribe suspicion to it.”

But the government case against Levandowski wasn’t just that

he checked out 14,000 files. The government argues that as a high-level manager, Levandowski had little legitimate reason to access the files in the first place. The feds say that his first and last checkout from the repository occurred in December 2015, weeks before his departure from Google. According to the government, he had to specifically request credentials to access the documents, and he copied all 14,000 files to his personal laptop a few days later.

"A grueling lesson in humility"

Along with his legal brief seeking clemency, Levandowski also included a personal letter to Judge William Alsup. Levandowski said he took full responsibility for his actions, but also noted that he had already suffered significantly from his actions.

"These last three and a half years have been a grueling lesson in humility, responsibility, and remorse, Levandowski said. "My professional reputation has been destroyed, my financial status has been obliterated, and I've lost many friends, partners, and colleagues as a result of my actions."

Levandowski's parents separated at a young age. As a young child, he lived in Belgium with his mother while his father moved back to California. His mother struggled to make ends meet. Levandowski writes that from a young age he felt a sense of responsibility as the "man of the house." This feeling of inadequacy stayed with him as an adult and he believes it contributed to his ferocious work ethic.

Levandowski says he now realizes that his hasty and acrimonious departure from Google was a mistake.

"I had many good years at Google working on world-changing technology that today we all take for granted," he wrote. "I understand now that my haste to leave Google, and my lack of clear communication created an open window for anger and

resentment to fester, and I am incredibly sorry to Larry Page, Sergey Brin, Sebastian Thrun, and my colleagues at Google for whom my abrupt departure was a slap in the face. I deeply regret the loss of those friendships."

Levandowski says that his new startup, a self-driving truck startup called Pronto, has been designed to uphold higher ethical standards. He notes that his new startup does not use lidar, the technology at the heart of his legal fight with Google.

Levandowski also argues that he can perform community service by speaking out about the harms that come from unethical business practices.

"There's a lot to be learned from my story, and I'm hopeful that I can share it in a way that it will be instructive to others and help the tech ecosystem evolve into one of fairness, equity, and justice," Levandowski writes. His lawyers have proposed that as part of Levandowski's community service, he "offer himself as an object lesson in what not to do, by candidly sharing the story of his misdeeds and speaking about the devastating consequences that followed."

https://arstechnica.com/?p=1695287