YouTube cracks down on QAnon conspiracists



Enlarge / Conspiracy theorist QAnon demonstrators protest child trafficking on Hollywood Boulevard in Los Angeles, California, August 22, 2020.
Kyle Grillot | Getty Images

reader comments

304 with 102 posters participating

Share this story

Google-owned YouTube has become the latest social media platform to crack down on the pro-Trump conspiracy theory QAnon ahead of November's US election, but stopped short of a full ban on the rapidly spreading movement.

In a blog post on Thursday, the video platform said that it would "prohibit content that targets an individual or group

with conspiracy theories that have been used to justify real-world violence," citing QAnon and related conspiracy theory Pizzagate.

The social media group also said that it had removed "tens of thousands" of videos and "hundreds of channels" related to QAnon, whose members believe US president Donald Trump is under threat from a Satanic "deep state" cabal of Democrats and Hollywood celebrities involved in child trafficking.

The move comes as Facebook and Twitter have also taken steps to eliminate the conspiracy theory from their platforms in recent months. In July, Twitter banned thousands of QAnon-related accounts and said it would stop recommending content linked to the movement, while Facebook announced plans to wipe it from its platform last week.

YouTube's recommendation algorithms have long been criticised for helping draw users towards radical and extremist content, as well as conspiracy theories. In response to allegations in 2018 that it was pushing its audience "down the rabbit hole" of often baseless conspiracy content, it updated its systems to restrict the reach of harmful misinformation.

Nevertheless, QAnon—which was labelled a domestic terror threat by the FBI last year—has continued to proliferate across social media platforms in the lead-up to the November election and taken on increasingly violent undertones, while also spilling into the mainstream.



Enlarge / A woman wearing a sweatshirt for the QAnon conspiracy theory gestures during a pro-Trump rally on October 11, 2020 in Ronkonkoma, New York.
Stephanie Keith | Getty Images

Left-leaning nonprofit Media Matters has identified 27 congressional candidates who have endorsed or given credence to QAnon, or promoted related content. Last month, a director in Citigroup's information technology department was dismissed after he was identified as the operator of one of the most important QAnon websites.

Instead of implementing a full ban, YouTube laid out several caveats to its changes: "content discussing [conspiracy theories] without targeting individuals or protected groups" will remain on the platform, it said, as well as news coverage of the issues.

The updates, introduced just weeks before the US vote, come as researchers have increasingly voiced frustration over what they see as a lack of transparency from YouTube over how much misinformation and co-ordinated manipulation is found on its platform, and how it is handled.

Others have pointed to lapses in the enforcement of existing policies. An external study by Media Matters, conducted before the announcement, found 17 top QAnon YouTube channels with more than 4.7 million subscribers “explicitly violated” its terms of service.

The move is likely to drive some QAnon believers towards a constellation of smaller alternative platforms with less stringent content moderation policies. Experts have also warned that members of the movement have already infiltrated less contentious communities, such as those dedicated to child protection, where they often attempt to win over new converts by presenting a less political version of the QAnon narrative.

YouTube said it would start enforcing the new policy immediately, adding that it would “look to ramp up in the weeks to come.”

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

https://arstechnica.com/?p=1715210

Twitter, Facebook face blowback after stopping circulation of NY Post story



reader comments

360 with 138 posters participating

Share this story

Facebook and Twitter today are facing criticism from all sides after taking rare action to suppress an apparent attempt at blatant disinformation being spread three weeks before the election.

Both social media platforms are deprecating or outright blocking the sharing of a link to a story the New York Post published this morning about Democratic presidential candidate Joe Biden. Although Twitter and Facebook have both acted in the past to deplatform fringe actors, today's action marks one of the extremely rare times either has taken action against a story from a relatively mainstream outlet.

The story

The story at the root of all the drama appears to be an attempt to duplicate the effect the Comey memo had on the 2016 presidential election by suggesting there's a scandal in the Biden camp. The New York Post claimed to have received copies of emails that were obtained from a laptop that Biden's son Hunter dropped off at a Delaware computer repair shop in 2019. These emails, which the Post called a "smoking gun," allegedly indicate that Hunter Biden connected his father with Ukrainian energy firm Burisma in 2014.

During President Donald Trump's impeachment trial earlier this year (yes, that was 2020, it only *feels* like a decade ago), Republican members of the House and Senate tried to paint Biden and Burisma as the "real" scandal, although there was no actual evidence of corruption. "Burisma" has remained something of a byword among a certain conservative segment ever since, particularly as Biden's standing in the polls has continued to improve.

The thin sourcing of the Post story almost immediately led to questions about its veracity. Disinformation expert Thomas Rid, a professor at Johns Hopkins University, laid out several of the red flags in the story in a lengthy Twitter thread shortly after it was published. "To journalists considering writing about this toxic story: don't—unless you can independently verify more details," Rid advised. "And even if you can verify something, acknowledge the possibility of disinformation up-front, especially against the backdrop of 2016. Not doing so is bad practice."

Other outlets immediately began to dig into the story. Business Insider determined it to be "riddled with holes and red flags." New York Magazine also wrote out the implausibilities in the Post's account. And The Daily Beast managed to track down and interview the owner of the computer

repair shop, who called Trump's impeachment a "sham" and alluded to the completely debunked conspiracy theory related to the 2016 murder of Seth Rich.

Biden campaign spokesman Andrew Bates denied the allegations in the Post's story, saying, "The New York Post never asked the Biden campaign about the critical elements of this story. They certainly never raised that Rudy Giuliani—whose discredited conspiracy theories and alliance with figures connected to Russian intelligence have been widely reported—claimed to have such materials. Moreover, we have reviewed Joe Biden's official schedules from the time and no meeting, as alleged by the New York Post, ever took place."

Social media's move

Facebook took action on the New York Post story before Twitter did. A little after 11:00 this morning, a Facebook spokesman confirmed on Twitter that Facebook was deprecating the story. He said, "While I will intentionally not link to the New York Post, I want [to] be clear that this story is eligible to be fact checked by Facebook's third-party fact checking partners. In the meantime, we are reducing its distribution on our platform."

"Reducing distribution" isn't the same as banning. Instead, it deprecates how likely Facebook's algorithm is to amplify content. Several other outlets and pages, including right-wing sites such as Breitbart, continued to share the allegations and links to the story throughout the day.

Twitter's first approach was to deprecate the story so it wouldn't float to the top of algorithmically managed content. By mid-afternoon, however, Twitter had gone one step further and outright banned *all* links to the story from being posted, either in the regular timeline or in direct messages.

Twitter representatives pointed press to the company's hacked

material policy, which prohibits sharing links to or images of hacked content. Twitter's guidelines for blocking URLs, which were updated this July, also include provisions for hacked material and content that "interferes with civic and election integrity."

Of course there's blowback

Conservative politicians, who already endlessly claim—with no evidence—that social media platforms suppress right-wing speech were, naturally, incensed.

Sen. Josh Hawley (R-Mo.) said in a tweet that he plans to ask the Federal Election Commission "whether this coordinated intervention by Facebook [and] Twitter for the Biden campaign constitutes a violation of campaign finance or other election laws." Hawley also sent letters to both Twitter and Facebook not only asking the sites to clarify their policies, but also demanding to know if anyone from the Biden campaign specifically asked for the story to be suppressed.

Neither were conservatives the only ones upset with Facebook's and Twitter's decision. Several observers, of every political stripe, argued that by banning the content, Facebook and Twitter instead ended up amplifying it in a textbook example of the Streisand effect. The New York Post certainly ran with the extra attention, publishing a follow-up story complaining about "censors" and the "suppression effort."

https://arstechnica.com/?p=1714926

Severed cable takes out Virginia voter site on registration deadline



Enlarge / Richmond, the capital of Virginia, looking scenic as seen from across the James River.

reader comments

249 with 127 posters participating, including story author

Share this story

Today is the last day to register to vote in the commonwealth of Virginia, so of course the official website for updating or managing voter registration is offline. Unlike in Florida, however, Virginia's site did not crash from high traffic but instead was rendered inaccessible because a vital fiber connecting the state's digital infrastructure was physically

cut.

Twitter users began to notice the state's voter registration page was failing to load sometime after 8:30 this morning, and at 9:00, the state's IT agency confirmed that a severed fiber optic cable was the root of all the problems.

"A fiber cut near Rt. 10 in Chester near the Commonwealth Enterprise Solutions Center (CESC) is impacting data circuits and virtual private network (VPN) connectivity for multiple Commonwealth agencies," the Virginia Information Technologies Agency wrote in a tweet, adding, "Technicians are on site and working to repair the cut; updates will be provided as work progresses."

In an update posted just before 1pm, VITA said the fiber was "inadvertently struck as part of activities related to a Chesterfield County roadside utilities project" but did not have an estimate for when repairs might be completed.

The severed cable affects not only voter registration, but also early in-person voting—underway across Virginia since September 18—in some jurisdictions because election officials use network-connected tablets to look up and verify voter information. Several other state systems have also been affected by the outage, including DMV operations, unemployment systems, and Virginia's COVID-19 dashboard and health information.

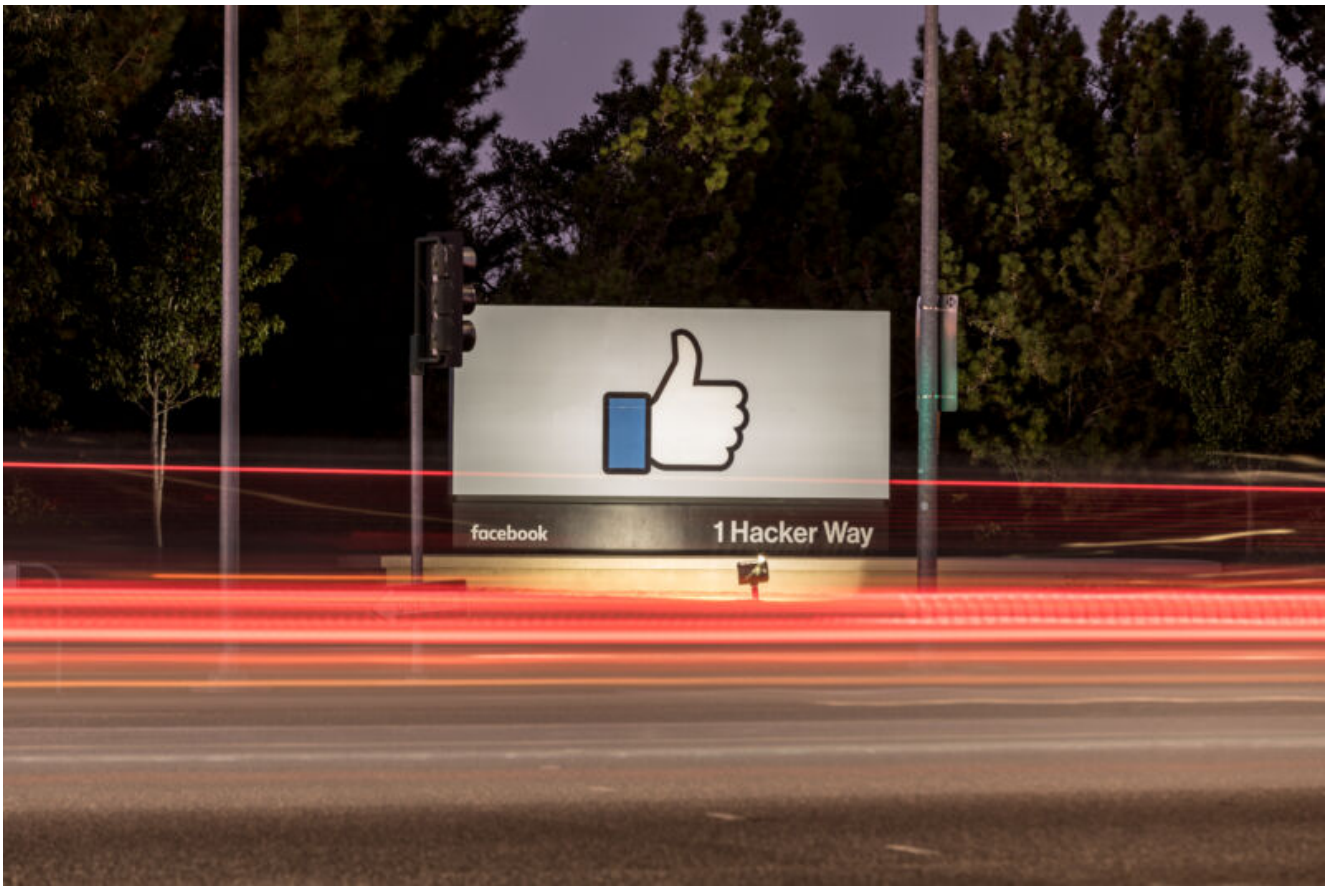
Virginia Lieutenant Governor Justin Fairfax called for the commonwealth to extend the voter registration deadline in light of the network failure. "We will work with the Administration to resolve this issue and ensure all voters have access to #Vote," Fairfax said in a tweet.

The outage is hopefully a temporary blip in an otherwise robust election season for the commonwealth. Thanks to a combination of pandemic concerns and expanded voter access laws that took effect on July 1, early in-person and mail-in

voting in Virginia this year has already smashed all previous records for the state. Almost 17 percent of all registered voters in Virginia, more than 975,000 individuals, had already cast their ballots as of October 11.

https://arstechnica.com/?p=1714010

Facebook bans Holocaust denial amid rapid rise in “deceptive” content



Enlarge / Facebook’s Menlo Park, California, headquarters as seen in 2017.

reader comments

170 with 92 posters participating

Share this story

Facebook today is, once again, theoretically ramping up enforcement against hate speech, this time with a new policy prohibiting Holocaust denial on the platform.

The change is due to a “well-documented rise in anti-Semitism globally,” Facebook executive Monika Bickert wrote in a corporate blog post today.

The policy is a complete 180 for Facebook CEO Mark Zuckerberg, who in a 2018 interview specifically described Holocaust denial as the kind of “deeply offensive” speech he nonetheless felt should be permitted on the platform. The next day, amid blowback, he “clarified” his position:

> *Our goal with fake news is not to prevent anyone from saying something untrue—but to stop fake news and misinformation spreading across our services. If something is spreading and is rated false by fact checkers, it would lose the vast majority of its distribution in News Feed. And of course if a post crossed line into advocating for violence or hate against a particular group, it would be removed. These issues are very challenging but I believe that often the best way to fight offensive bad speech is with good speech.*

Zuckerberg said in a Facebook post today that his own thinking “has evolved” amid the growth in anti-Semitic violence in recent years. “Drawing the right lines between what is and isn’t acceptable speech isn’t straightforward,” he added, “but with the current state of the world, I believe this is the right balance.”

The ban on Holocaust denial is just the latest in a huge suite

of policy changes and proposals Facebook has made in the past two weeks explicitly related to hate speech, misinformation, or “influence operations.”

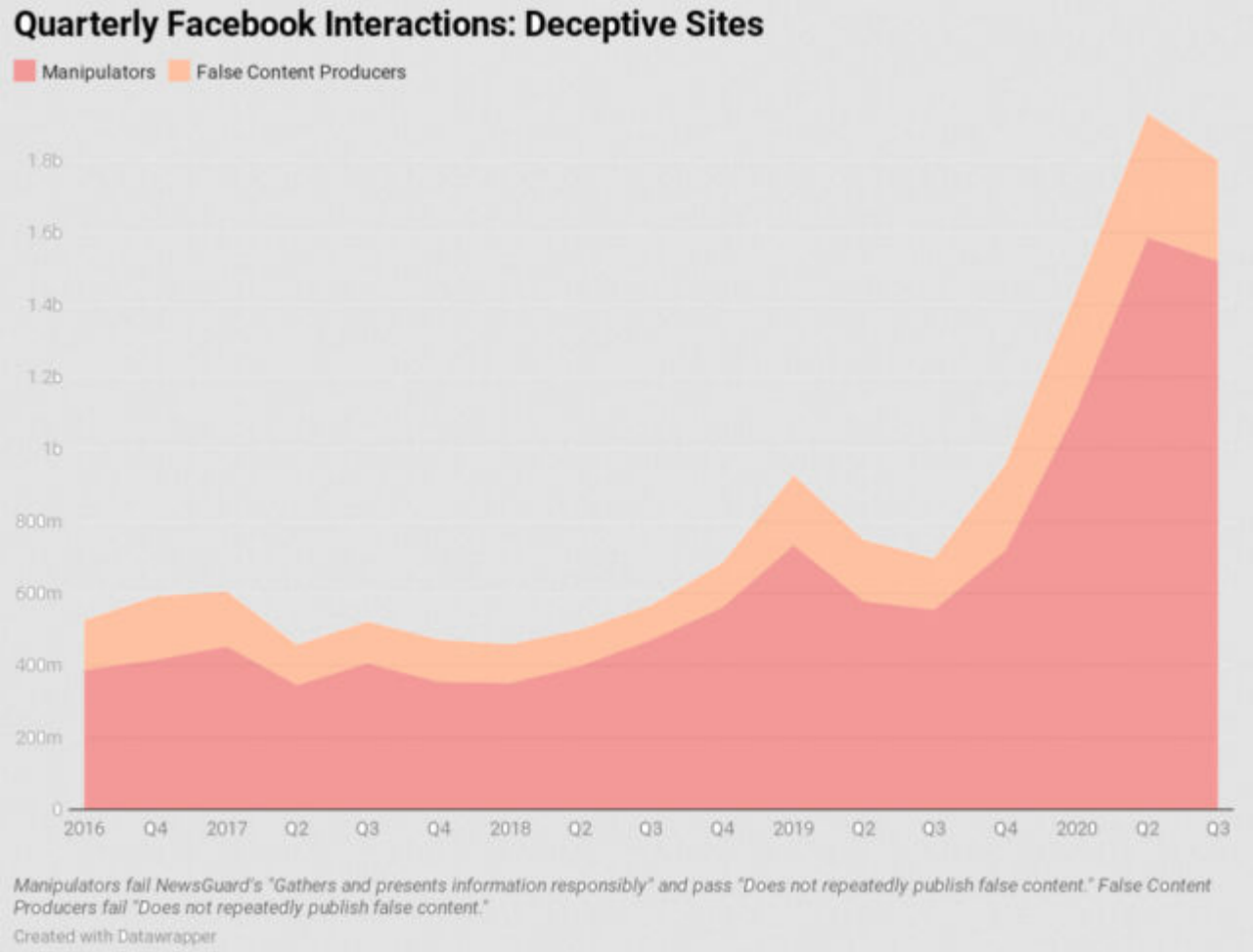
After all this time, why now?

Previous much-publicized efforts by Facebook to reduce hate speech and misinformation on the platform have not gone particularly well overall, and the world is still dealing with the effects of how quickly and widely misinformation can spread thanks to social media. A new study released today finds that the problem is getting rapidly worse, not better.

The digital project arm of the German Marshall Fund, a nonpartisan think tank, published a report today finding that Facebook has not only failed to limit the spread of false claims on its platform but instead has allowed disinformation to more than double since 2016.

The study ranks the number of interactions that come from what the GMF calls “deceptive sites,” which fall into two broad categories. The first category includes sites that “repeatedly published content that is provably false” and is conveniently called “false content producers.” The second, larger group of sites, called “manipulators,” technically doesn’t usually run wholly untrue stories but instead “egregiously distort[s] or misrepresent[s] information to make an argument.”

Facebook engagement with both kinds of deceptive sites has increased 242 percent since this time in 2016, GMF found, with the vast majority of that growth happening in the past year, since the third quarter of 2019. Interactions with outright false content have just about doubled, but interactions with “manipulator” sites have increased by close to 300 percent.



Enlarge / A graph created by the German Marshall Foundation Digital New Deal project shows a *dramatic* increase in Facebook engagement with deceptive sites since the run-up to the 2016 US presidential election.

The study includes more than 720 sites under the "deceptive" umbrella, but GMF found that the top 10 sites alone account for a whopping 62 percent of all the interactions they tracked, with the remaining 711 sites all together accounting for the remaining 38 percent. All of the top 10 qualified as "manipulator" sites, including Breitbart and The Daily Wire. Although the top sites all skew conservative, GMF noted, the study includes both left-leaning and non-political deceptive sites as well.

The perennially popular Fox News, which garnered the most interactions of any of the sites included in the study, also qualified under the "manipulator" label. The research team finds that Fox has published "irresponsible and misleading claims," particularly related to COVID-19. At the same time,

Fox rated more highly than other outlets in the “manipulator” category because it follows journalistic practices such as correcting errors, avoiding deceptive headlines, labeling advertising, and disclosing ownership.

The misinformation spread by deceptive sites is a key part of what GMF calls the “disinformation supply chain,” which, as we learned in 2016, can have major real-world effects. Such articles are designed to push emotional hot buttons, and Facebook’s algorithms then amplify that content to more users, and the cycle goes on.

“Disinformation is infecting our democratic discourse at rates that threaten the long-term health of our democracy,” said Karen Kornbluh, the director of GMF Digital and head of the project. “A handful of sites masquerading as news outlets are spreading even more outright false and manipulative information than in the period around the 2016 election. This data underscores that de-amplifying—or adding friction to the spread of—content from a handful of the most dangerous sites could dramatically decrease disinformation online.”

https://arstechnica.com/?p=1713541

FBI/DHS: Government election systems face threat from active Zerologon exploits



Getty Images

reader comments

29 with 25 posters participating

Share this story

The FBI and the cybersecurity arm of the Department of Homeland Security said they have detected hackers exploiting a critical Windows vulnerability against state and local governments and that in some cases the attacks are being used to breach networks used to support elections.

Members of unspecific APTs—the abbreviation for advanced persistent threats—are exploiting the Windows vulnerability dubbed Zerologon. It gives attackers who already have a toehold on a vulnerable network access to the all-powerful domain controllers that administrators use to allocate new accounts and manage existing ones.

To gain initial access, the attackers are exploiting separate

vulnerabilities in firewalls, VPNs, and other products from companies including Juniper, Pulse Secure, Citrix NetScaler, and Palo Alto Networks. All of the vulnerabilities—Zerologon included—have received patches, but as evidenced by Friday's warning from the DHS and FBI, not everyone has installed them. The inaction is putting governments and elections systems at all levels at risk.

Officials wrote:

> *This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks. Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.*
>
> *CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.*

Zerologon works by sending a string of zeros in a series of messages that use the Netlogon protocol, which Windows servers rely on for a variety of tasks, including allowing end users to log in to a network. People with no authentication can use the exploit to gain domain administrative credentials, as long as the attackers have the ability to establish TCP connections with a vulnerable domain controller. The requirement to establish TCP connections with the domain controller is likely why attackers are chaining Zerologon with exploits of VPNs and firewalls.

Friday's advisory provides some guidance for organizations that think they have or may have been compromised. The most

important takeaway is that the targeted vulnerabilities—some that have been available for more than a year — should be applied or the hardware they run should be disconnected from their networks.

https://arstechnica.com/?p=1713241

Microsoft thumbs its nose at Apple with new “app fairness” policy



Enlarge / Microsoft sign at the entrance of their Silicon Valley campus in Mountain View, California.

reader comments

198 with 112 posters participating

Share this story

Microsoft this week adopted a whole slew of “fairness principles” for its Windows app store. The list of principles does look like a decent set of guidelines for both consumers and developers—but it also looks a whole lot like Microsoft is taking the metaphorical ball, throwing it at Apple’s face, and daring their iCompetitor to make the next move.

The principles, which Microsoft listed in a corporate blog post, essentially promise that Windows will keep on doing what it already does with regard to app distribution, interoperability, payment systems, and everything else.

The first item, for example, promises that developers may choose whether to distribute Windows programs through the Microsoft Store or through their own competing app storefronts. This has always been the case, and it’s why Steam, the Epic Games store, and every other Windows software distribution method exist. Windows also promises not to block an app from Windows “based on a developer’s choice of which payment system to use” for processing in-app purchases which, again, is why and how both Web-based and app-based digital software storefronts for Windows exist.

“Windows 10 is an open platform. Unlike some other popular digital platforms, developers are free to choose how they distribute their apps,” Microsoft said. “The Microsoft Store is one way… But there are other popular and competitive alternatives on Windows 10.”

The company specifically gave a shoutout to game distributors, adding, “Third-party app stores, such as those from Steam and Epic, are available for Windows and offer developers different pricing (or revenue share) options, standards, requirements

and features.” Microsoft’s principles are “designed to preserve this freedom of choice, and the robust competition and innovation that it enables on Windows 10.”

The trillion-ton Apple in the room

The blog post never once mentions Apple, but it is impossible to read Microsoft’s declaration as anything other than a shot across Apple’s bow. Microsoft said explicitly that its principles draw on work by the Coalition for App Fairness, a trade group that came together in September to push for changes to the App Store policies. That coalition’s founding members include companies such as Basecamp, Spotify, and Epic, all of whom have had extremely public fights with Apple over its policies in recent months.

The developers who have challenged Apple argue that the company is doing the exact opposite of what Microsoft just promised to keep doing. Apple requires developers to distribute iOS apps through the App Store, with no exceptions. It requires developers to use its own in-app payment system, with no exceptions. And it takes a 30 percent cut of all those transactions—except there are some exceptions for companies with enough clout to demand it such as Amazon and Netflix.

Competitors are not the only ones frustrated with Apple’s behavior. A Congressional committee this week published a blockbuster report arguing that the way Apple ties its App Store and in-app payments mechanisms together falls afoul of antitrust law and is anticompetitive.

Microsoft, meanwhile, seems to have an immediate interest in elbowing its way onto iOS devices. The company hinted this week that it plans to use a browser-based workaround to get Project xCloud, its in-game streaming service, onto iPhones.

The silent “X”

The Windows-native app store is not particularly integral to the PC experience for most users, no matter how hard Microsoft tries to promote it. Microsoft didn’t introduce the platform in its current incarnation until the launch of Windows 8 in 2012, and by that time both individual consumers and enterprise buyers had almost 30 years of practice acquiring their Windows programs elsewhere. (And some of Microsoft’s previous attempts, such as the ill-fated Games for Windows Live, actively drove users to competitors such as Steam by being, well, kind of terrible.)

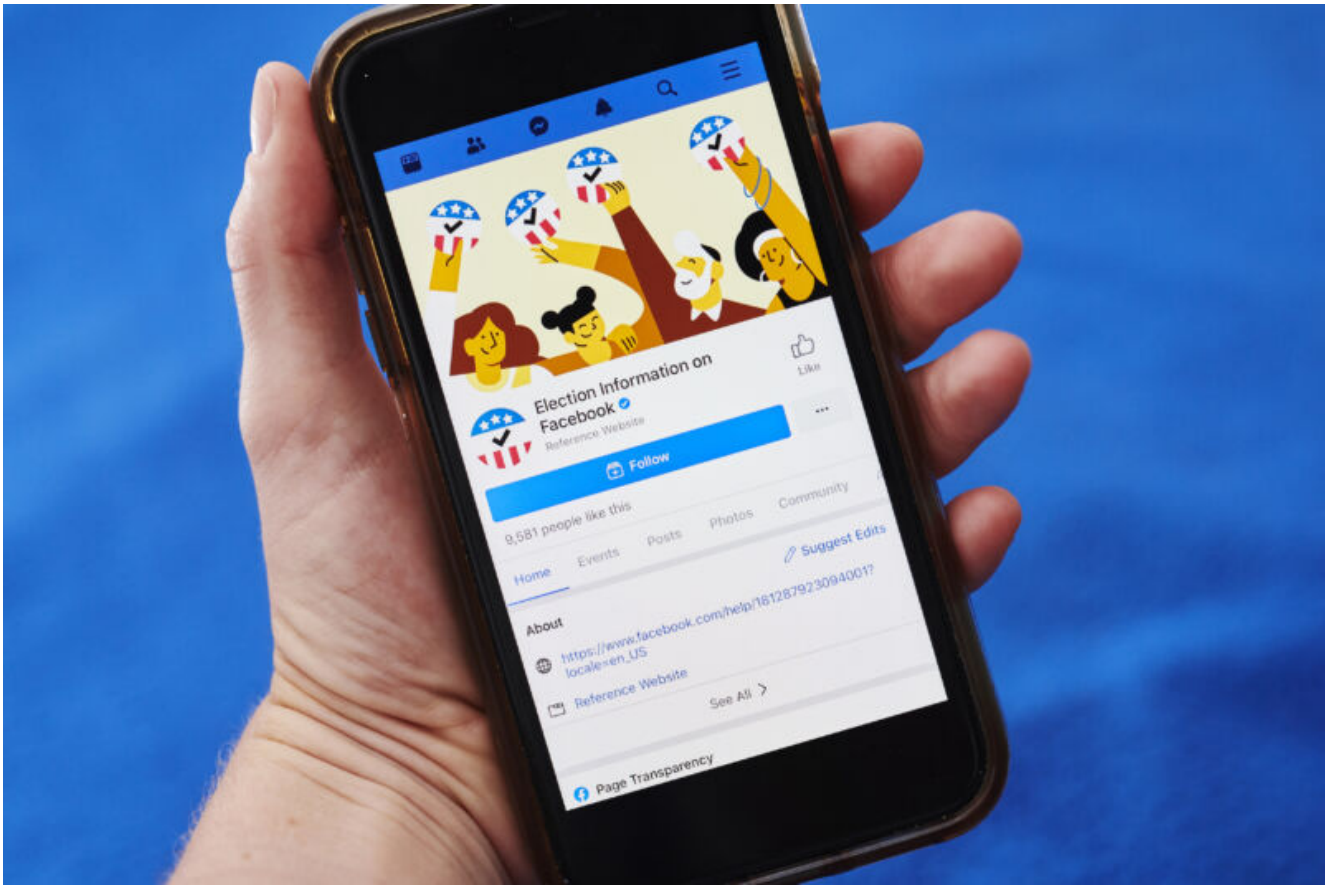
But Microsoft in its blog post does indeed realize that it has *two* major app stores to its name, and the company admits that its new rules for “fairness” do not apply equally to both of them. The Xbox online store works much more like the iOS App Store than it does like software distribution for Windows. Companies like Epic have to fork over 30 percent of their take for in-game purchases to Microsoft for Xbox players just as they do to Apple, Google, or Sony for iOS, Android, or PlayStation players.

“It’s reasonable to ask why we are not also applying these principles to [the] Xbox store today,” Microsoft said. Instead of answering that question outright, however, Microsoft punted to an indeterminate future.

“Game consoles are specialized devices optimized for a particular use. Though well-loved by their fans, they are vastly outnumbered in the marketplace by PCs and phones,” Microsoft said, as if that means that developers particularly care about the difference when it comes to that 30 percent cut. Given the “fundamental differences” between the PC and set-top console market, Microsoft said, “we have more work to do to establish the right set of principles for game consoles.”

https://arstechnica.com/?p=1713047

Facebook to pause all political advertising—after the election



Enlarge / Facebook's "voter information center" as seen in July 2020.

reader comments

132 with 60 posters participating

Share this story

It seems fair to say that, here in the United States, this is an election season unlike any other, with tensions running exceptionally high. Facebook, which through its collection of apps reaches the vast majority of the US population, has again launched a new slew of initiatives to mitigate the harm misinformation on its platforms can cause. Several of these measures are sound ideas, but unfortunately, two of its latest efforts once again amount to waiting until the horse has made it halfway around the world before you shut the barn door.

Facebook explained yesterday in a corporate blog post what its Election Day efforts are going to look like on both Facebook and Instagram. The company has promised for months that it will run real-time fact-checking on and after November 3 to prevent any candidate from declaring victory before a race is actually called, and it showed what that process will look like.

In that post, Facebook also said that although ads are "an important way to express voice," it plans to enact a temporary moratorium on "all social issue, electoral, or political ads in the US" *after* the polls close on November 3, to "reduce opportunities for confusion or abuse." That stance will put Facebook, at least for the time being, in like with Twitter's position on political ads.

Too late?

Confusion and abuse, however, are already rampant. For the last year, Facebook has maintained an infamously hands-off stance when it comes to fact-checking political advertising. The platform has occasionally intervened, usually after media pressure, when those ads cross the line of one of its other policies. In June, for example, Facebook pulled a line of Trump campaign ads for using Nazi imagery, and in September it pulled another batch of Trump campaign ads for targeting

refugees. Other ads, however—including deceptively manipulated photos and videos of Democratic presidential candidate Joe Biden—have been left alone.

Facebook is also prohibiting content that calls for "militarized" poll-watching and voter intimidation, as the Trump campaign ramps up rhetoric calling for supporters "to go into the polls and watch very carefully." That policy, however, only applies to new content posted going forward and not to content that has already gone viral.

Unfortunately, such content has already generated millions of views. Donald Trump Jr. in September posted a video to Facebook calling for an "Army for Trump" to defend against alleged widespread election fraud efforts by the Democratic Party. (No evidence of any such effort exists, and while there are documented instances of election fraud in recent years, it is extremely rare.)

"We need every able-bodied man and woman to join Army for Trump's election security operation," Trump Jr. says in the video, encouraging viewers to "enlist now." Although that video very clearly breaks the new rules, however, it's not going anywhere.

"When we change our policies, we generally do not apply them retroactively," Facebook executive Monika Bickert said. "Under the new policy, if that video were to be posted again, we would indeed be removing it."

Concerns about a rise in violence leading up to the election are, sadly, not unfounded. Just this morning, for example, the FBI announced it had intercepted a plot by five Michigan men and one Delawarean to kidnap Michigan Gov. Gretchen Whitmer and "overthrow" the state government, which was in part coordinated on Facebook and other social media platforms.

Coordinated response

It seems clear that social media platforms, acting alone, cannot sufficiently address the threat of coordinated disinformation. Facebook today said as much when outlining a set of proposals for new regulation or legislation that would apply to both it and other social platforms.

“If malicious actors coordinate off our platforms, we may not identify that collaboration,” Facebook head of security policy Nathaniel Gleicher wrote. “If they run campaigns that rely on independent websites and target journalists and traditional media, we and other technology companies will be limited to taking action on the components of such campaigns we see on our platforms. We know malicious actors are in fact doing both of these things… There is a clear need for a strong collective response that imposes a higher cost on people behind influence operations in addition to making these deceptive campaigns less effective.”

Today, for example, Facebook said it removed 200 fake accounts that were tied to a marketing firm that worked on behalf of two US conservative political action groups, Turning Point USA and Inclusive Conservation Group. The marketing firm is now banned from Facebook, but clearly most of the coordination its employees did would have taken place using tools other than Facebook, and its networks of fake accounts and disinformation may still be active on other platforms.

“Regulations can be powerful tools in our collective response to these deceptive campaigns,” Facebook said, recommending seven key principles. Chief among them are transparency and collaboration: companies should agree to share threat signals across “platforms, civil society, and government, while protecting the privacy of innocent users who may be swept up in these campaigns,” Facebook suggested.

But Facebook also wants help from the law in the form of

actual consequences for conducting certain kinds of influence operations. The company is asking regulators to “impose economic, diplomatic and/or criminal penalties” on the entities that organize these disinformation campaigns.

https://arstechnica.com/?p=1712653

House: Amazon, Facebook, Apple, Google have “monopoly power,” should be split



Enlarge / The United States Capitol Building, the seat of Congress, on the National Mall in Washington, DC.

reader comments

177 with 95 posters participating, including story author

Share this story

Last June, the House Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law began an in-depth investigation into four major firms—Amazon, Apple, Facebook, and Google. The subcommittee wanted to answer one key question: did Big Tech get big playing by the rules, or does it cheat to stay at the top? After 16 months of hearings, research, and analysis, the panel's findings are out… and the results look really bad for every company involved.

The tech sector does indeed suffer from abuses of "monopoly power," the subcommittee concluded in the mammoth 450-page report (PDF) published late yesterday afternoon.

"As they exist today, Apple, Amazon, Google, and Facebook each possess significant market power over large swaths of our economy. In recent years, each company has expanded and exploited their power of the marketplace in anticompetitive ways," Judiciary Committee Chairman Jerrold Nadler (D-N.Y.) and antitrust subcommittee Chairman David Cicilline (D-R.I.) said in a joint statement. "Our investigation leaves no doubt that there is a clear and compelling need for Congress and the antitrust enforcement agencies to take action that restores competition, improves innovation, and safeguards our democracy."

What was Congress looking for?

As we've explained before, antitrust law isn't just about monopolies. Being the largest player in a sector—even if you're so big you dwarf any potential competition—isn't inherently unlawful. Sometimes that can just be the way a market shakes out.

Antitrust law is instead concerned with what you did to become dominant and what you do with the outsized power that comes from being the biggest. If you have a 90 percent market share but it all came from natural growth and you deal fairly with other companies and with consumers, antitrust regulators are probably going to leave you alone. But if nascent startups can demonstrate you used your bulk to knock them out before they could become real competition, or if competitors can show you unfairly leveraged different parts of your business to squeeze them out? *Those* are problems.

After conducting seven hearings, reviewing more than 1.3 million internal documents, conducting more than 240 interviews, and reviewing submissions from 38 antitrust experts, the committee found evidence that all four companies have acted anticompetitively and are continuing to do so today.

Amazon: It’s the everything

Amazon is dominant in online sales, the committee found. Between its first-party sales and its third-party marketplace, Amazon controls roughly 50 percent of the US e-commerce market and a much higher percentage in certain sectors, such as e-books. And the company uses that gatekeeper, monopoly power unfairly, the committee concluded.

Amazon leverages its power on both sellers and manufacturers to break agreements, push for unfairly favorable terms in negotiations, and lock would-be competitors into its ecosystem, the report concluded. The problems were particularly pronounced in the company’s third-party marketplace. Roughly 2.3 million vendors worldwide sell their goods through Amazon’s marketplace, and of those, just over a third “rely on Amazon as their sole source of income.” In other words, Amazon *is* their storefront, and Amazon uses that leverage to twist metaphorical arms whenever it likes.

“Numerous sellers told Subcommittee staff in interviews that they cannot turn to alternative marketplaces, regardless of how much Amazon may increase their costs of doing business or how badly they are treated,” the report reads. “Sellers feel forced to be on Amazon because that is where the buyers are.”

And of course, Amazon is *also* a retailer, and in many categories of goods, it competes directly with the sellers for whom it is providing infrastructure. It hoovers up data from third-party sales to inform its own product launches, then it competes directly with the merchants who are relying on it for their livelihood. It also operates a logistics business that it strong-arms those sellers into using by allowing its opaque “buy box” algorithm to penalize sellers who don’t.

Amazon also behaved anticompetitive around several of its dozens of acquisitions over the past decade, the committee found. Not only have these purchases led to less consumer choice and vastly expanded Amazon’s trove of consumer data, but in at least one case, Amazon used predatory pricing to undercut and eventually acquire a rival firm anticompetitively.

The report finds that Amazon continues to leverage its power up and down the chain to make the costs of walking away from it too high for most businesses and consumers—in antitrust terms, these are called switching costs and network effects. “Amazon expanded its market power through avoiding taxes, extracting state subsidies, and engaging in anticompetitive conduct—tactics that have given the company an unfair advantage over actual and potential competitors,” the report concludes. “Amazon’s market power is durable and unlikely to erode in the foreseeable future.”

Apple: It’s the App Store

Apple controls about 45 percent of the US smartphone market and 20 percent of the global smartphone market, the committee

found, and is projected to sell its 2 billionth iPhone in 2021. It is correct that, in the smartphone handset market, Apple is *not* a monopoly. Instead, iOS and Android hold an effective duopoly in mobile operating systems.

However, the report concludes, Apple *does* have a monopolistic hold over what you can *do* with an iPhone. You can only put apps on your phone through the Apple App Store, and Apple has total gatekeeper control over that App Store—that's what Epic is suing the company over.

That monopoly control allows Apple to "generate supra-normal profits" from the App Store, the report finds, and those profits have become a dramatically higher percentage of Apple's revenue over time, now generating billions more than the company spends annually to run the App Store.

Apple also ties its in-app payment system (IAP) to the app store in an anticompetitive way, the committee found. Citing internal Apple communications as well as testimony from the founders of ProtonMail and Hey, among others, the report finds that "Apple has leveraged its power over the App Store to require developers to implement IAP or risk being thrown out of the App Store."

Using IAP raises costs for developers, several testified. For apps that compete directly against Apple's own first-party services, they said, paying Apple for the privilege of making less money doesn't make economic sense—that's the heart of Spotify's complaint against Apple. But developers also say they can't leave iOS, because although iPhone users are a minority of the market, they tend by and large to have more money and be bigger spenders than Android users. (Several of these developers joined together earlier this fall to launch a trade group pushing for Apple to lower its fees and untie the App Store from IAP.)

The committee found internal documents showing that company

leadership, including former CEO Steve Jobs, “acknowledged that IAP requirement would stifle competition and limit the apps available to Apple’s customers.” The report concludes that Apple has also unfairly used its control over APIs, search rankings, and default apps to limit competitors’ access to iPhone users.

Facebook: It’s the acquisitions (and the data)

Facebook outright “has monopoly power in the market for social networking,” the report concludes, and that power is “firmly entrenched and unlikely to be eroded by competitive pressure” from anyone at all due to “high entry barriers—including strong network effects, high switching costs, and Facebook’s significant data advantage—that discourage direct competition by other firms to offer new products and services.”

Facebook alleges that it competes heavily for users with other platforms such as Twitter, TikTok, Snapchat, and Pinterest. But it doesn’t compete with other major platforms, such as Instagram, because it bought them up before they could become real competition. The company’s top four apps, taken together—Facebook, Instagram, Messenger, and WhatsApp—comprise four of the seven most-popular mobile apps inside the United States. Facebook’s flagship app alone reaches 200 million US users, or 74 percent of smartphone users.

That reach alone keeps people using the product. There’s a high switching cost for social media platforms because users want to go where their friends are. “Either everyone uses them, or no-one uses them,” an internal Facebook document concluded. Facebook also hides its data portability settings from users, the report concluded, which leads users to keep their accounts active so they don’t lose information such as photo albums.

Merger review is supposed to guarantee that you can't buy out your rivals if doing so would severely reduce competition in the sector. For example, if Company A has 40 percent of the market, Company B has 10 percent of the market, and company C has 50 percent of the market, Companies A and B could probably merge, and Company C might be able to acquire Company B, but Companies A and C would not be allowed to merge because the combined company would then have a 90 percent market share. Competition in the sector would be destroyed.

So many acquisitions

But regulators did not block Facebook's blockbuster acquisitions of either Instagram or WhatsApp, and they didn't stop 60 other Facebook acquisitions. This led to what one former employee described to the committee as collusion between the platforms, "but with an internal monopoly." The employee added: "If you own two social media utilities, they should not be allowed to shore each other up. It's unclear to me why this should not be illegal. You can collude by acquiring competitors and forbidding competition."

Facebook used some of those acquisitions, such as the VPN service Onavo, to gather nonpublic data on other firms' apps and then use that data to further inform its own acquisition strategy. Snapchat legendarily maintained a dossier, called "Project Voldemort," on Facebook's attempts to undercut Snapchat's business and acquire the firm at a cut rate.

This strategy was deliberate, the committee found. As evidence, the report cited internal communications from Facebook CEO Mark Zuckerberg and other company leadership. "Facebook's serial acquisitions reflect the company's interest in purchasing firms that had the potential to develop into rivals before they could fully mature into strong competitive threats," it concludes.

Facebook also used acquisitions, such as its purchase of ad

service Atlas from Microsoft, to expand its grasp on consumer data and become a major player in the online advertising market, where it now dominates. “Notwithstanding Google’s dominance,” the committee wrote, “market participants interviewed by the subcommittee consider Facebook ‘unavoidable’ or ‘must have’ due to the reach and scale of its platform.”

Together with Google, Facebook is one half of a duopoly that controls online advertising to the detriment of competition, the committee concluded.

https://arstechnica.com/?p=1712319

Facebook bans QAnon entirely, says previous crackdown wasn’t enough



Enlarge / Supporters of President Donald Trump wearing “QAnon” T-shirts wait in line before a campaign rally at Freedom Hall on October 1, 2018, in Johnson City, Tennessee.

reader comments

110 with 66 posters participating

Share this story

Facebook is banning the QAnon conspiracy-theorist group, expanding on a policy that previously led to the removal of over 1,500 QAnon-related pages and groups.

Starting in mid-August, Facebook removed QAnon pages and groups that contained discussions of potential violence. Today, Facebook said, “We believe these efforts need to be strengthened when addressing QAnon,” and the company strengthened the ban so that it applies regardless of whether the pages and groups discuss violence.

Facebook wrote:

> *Starting today, we will remove any Facebook Pages, Groups and Instagram accounts representing QAnon, even if they contain no violent content. This is an update from the initial policy in August that removed Pages, Groups and Instagram accounts associated with QAnon when they discussed potential violence while imposing a series of restrictions to limit the reach of other Pages, Groups and Instagram accounts associated with the movement… We are starting to enforce this updated policy today and are removing content accordingly, but this work will take time and need to continue in the coming days and weeks.*

Facebook said its earlier removal of 1,500 QAnon pages and groups was accompanied by the removal of another 6,500 pages and groups that were "tied to more than 300 Militarized Social Movements." Facebook said it will continue to disable the profiles of admins who manage pages and groups that were removed for violating the policy.

New problems popped up after initial ban

Facebook said that "several" problems led to today's policy update:

> *For example, while we've removed QAnon content that celebrates and supports violence, we've seen other QAnon content tied to different forms of real-world harm, including recent claims that the west coast wildfires were started by certain groups, which diverted attention of local officials from fighting the fires and protecting the public. Additionally, QAnon messaging changes very quickly and we see networks of supporters build an audience with one message and then quickly pivot to another. We aim to combat this more effectively with this update that strengthens and expands our enforcement against the conspiracy theory movement.*

This may not be the last policy update, Facebook said. “We expect renewed attempts to evade our detection, both in behavior and content shared on our platform, so we will continue to study the impact of our efforts and be ready to update our policy and enforcement as necessary,” the company said.

Facebook said it has its “Dangerous Organizations Operations” team on the case. The group consists of specialists who “proactively detect content for removal,” a method that “has provided better leads in identifying new evolutions in violating content than sifting through user reports.”

Twitter has taken similar action against QAnon.

As NBC News writes, the QAnon conspiracy theory “posits that high-profile Democrats and Hollywood celebrities are members of a child-eating cabal that is being secretly taken down by President Donald Trump, and that members of this fictitious cabal will soon be marched to their execution.” QAnon accounts pushed the baseless claim that Democratic presidential nominee Joe Biden would secretly wear an earpiece in a debate against President Trump, and they also “pushed the conspiracy theory that Trump is not sick with the coronavirus, but carrying out secret missions in a fictitious war that has been predicted by QAnon followers,” NBC News wrote. QAnon accounts have also been spreading disinformation about COVID-19 in general.

https://arstechnica.com/?p=1712320

Last-minute requests

reportedly crush Florida voter registration site



Enlarge / A Florida man wears a sticker indicating that he registered to vote.

reader comments

143 with 70 posters participating

Share this story

Florida’s secretary of state has extended the deadline for voter registration to 7pm today. Registration officially closed last night at midnight, but problems with the state’s website prevented some Floridians from completing their registration in time.

Laurel Lee, the Florida secretary of state appointed by Republican Gov. Ron DeSantis, announced the change after noon

on Tuesday, giving voters who missed the previous deadline less than seven hours to try again.

Voting rights advocates sued Lee on Tuesday morning, arguing that the website problems had deprived Floridians of their right to vote. They pointed out that Florida's voter registration website has a history of crashing under heavy loads.

The lawsuit says that Florida officials were repeatedly warned that the problem was likely to recur as the deadline neared. But according to the plaintiffs, officials did little to address the problem, and the critics' concerns were vindicated. A number of voters encountered problems with the site in the hours before the midnight deadline.

Indeed, documents obtained by the government transparency group American Oversight demonstrate that this year's registration fiasco is a rerun of problems the state suffered during the 2018 election cycle. That year, numerous users submitted feedback to Florida officials reporting that website problems had prevented them from registering. "THIS IS RIDICULOUS," one voter wrote in a July 2018 email thread with state officials.

In a follow-up legal filing today, the plaintiffs argued that the 7pm deadline provides "woefully insufficient time to educate voters and allow them to use" the state's voter registration system. "Voters who are busy with work and caregiving responsibilities need additional time to make the opportunity to register to vote at all meaningful," the plaintiffs wrote.

They are seeking an extension until midnight on the second day after a court ruling. That would give voters at least 48 hours to complete the registration process. The court has scheduled a hearing on the issue for 8:30am on Wednesday morning.

As I write this, Florida voters have about three more hours to

register—assuming the deadline isn’t extended again. If you’re an unregistered Floridian, you can register here or visit a local voter registration office.

https://arstechnica.com/?p=1712252