



FOREIGN AFFAIRS

How to Save Democracy From Technology

Ending Big Tech's Information Monopoly

BY FRANCIS FUKUYAMA, BARAK RICHMAN, AND ASHISH GOEL
January/February 2021

FRANCIS FUKUYAMA is a Senior Fellow at Stanford University's Freeman Spogli Institute for International Studies.

BARAK RICHMAN is Katharine T. Bartlett Professor of Law and Professor of Business Administration at Duke University School of Law.

ASHISH GOEL is Professor of Management Science and Engineering at Stanford University.

They are members of the Working Group on Platform Scale for Stanford University's Program on Democracy and the Internet.

Among the many transformations taking place in the U.S. economy, none is more salient than the growth of gigantic Internet platforms. Amazon, Apple, Facebook, Google, and Twitter, already powerful before the COVID-19 pandemic, have become even more so during it, as so much of everyday life moves online. As convenient as their technology is, the emergence of such dominant corporations should ring alarm bells—not just because they

hold so much economic power but also because they wield so much control over political communication. These behemoths now dominate the dissemination of information and the coordination of political mobilization. That poses unique threats to a well-functioning democracy.

While the EU has sought to enforce antitrust laws against these platforms, the United States has been much more tepid in its response. But that is beginning to change. Over the past two years, the Federal Trade Commission and a coalition of state attorneys general have initiated investigations into potential abuses of these platforms' monopoly power, and in October, the Justice Department filed an antitrust suit against Google. Big Tech's critics now include both Democrats who fear manipulation by domestic and foreign extremists and Republicans who think the large platforms are biased against conservatives. Meanwhile, a growing intellectual movement, led by a coterie of influential legal scholars, is seeking to reinterpret antitrust law to confront the platforms' dominance.

Although there is an emerging consensus about the threat that the Big Tech companies pose to democracy, there is little agreement about how to respond. Some have argued that the government needs to break up Facebook and Google. Others have called for more stringent regulations to limit these companies' exploitation of data. Without a clear way forward, many critics have defaulted to pressuring platforms to self-regulate, encouraging them to take down dangerous content and do a better job of curating the material carried on their sites. But few recognize that the political harms posed by the platforms are more serious than the economic ones. Fewer still have considered a practical way forward: taking away the platforms' role as gatekeepers of content. This approach would entail inviting a new group of competitive "middleware" companies to enable users to

choose how information is presented to them. And it would likely be more effective than a quixotic effort to break these companies up.

PLATFORM POWER

Contemporary U.S. antitrust law has its roots in the 1970s, with the rise of free-market economists and legal scholars. Robert Bork, who was solicitor general in the mid-1970s, emerged as a towering scholar who argued that antitrust law should have one and only one goal: the maximization of consumer welfare. The reason some companies were growing so large, he argued, was that they were more efficient than their competitors, and so any attempts to break up these firms were merely punishing them for their success. This camp of scholars was informed by the laissez-faire approach of the so-called Chicago school of economics, led by the Nobel laureates Milton Friedman and George Stigler, which viewed economic regulation with skepticism. The Chicago school argued that if antitrust law should be structured to maximize economic welfare, then it ought to be highly restrained. By any standard, this school of thought was an astounding success, influencing generations of judges and lawyers and coming to dominate the Supreme Court. The Reagan administration's Department of Justice embraced and codified many tenets of the Chicago school, and U.S. antitrust policy has largely settled on a lax approach ever since.

After decades of dominance of the Chicago school, economists have had ample opportunity to evaluate the effects of this approach. What they have found is that the U.S. economy has grown steadily more concentrated across the board—in airlines, pharmaceutical companies, hospitals, media outlets, and, of course, technology companies—and consumers have suffered. Many, such as Thomas Philippon, explicitly link higher prices in the United States, compared with those in Europe, to inadequate antitrust enforcement.

Now, a growing “post-Chicago school” argues that antitrust law should be enforced more vigorously. Antitrust enforcement is necessary, they believe, because unregulated markets cannot stop the rise and entrenchment of anticompetitive monopolies. The shortcomings of the Chicago school’s approach to antitrust have also led to the “neo-Brandeisian school” of antitrust. This group of legal scholars argues that the Sherman Act, the country’s early federal antitrust statute, was meant to protect not just economic values but also political ones, such as free speech and economic equality. Since digital platforms both wield economic power and control communication bottlenecks, these companies have become a natural target for this camp.

It is true that digital markets exhibit certain features that distinguish them from conventional ones. For one thing, the coin of the realm is data. Once a company such as Amazon or Google has amassed data on hundreds of millions of users, it can move into completely new markets and beat established firms that lack similar knowledge. For another thing, such companies benefit greatly from so-called network effects. The larger the network gets, the more useful it becomes to its users, which creates a positive feedback loop that leads a single company to dominate the market. Unlike traditional firms, companies in the digital space do not compete for market share; they compete for the market itself. First movers can entrench themselves and make further competition impossible. They can swallow up potential rivals, as Facebook did by purchasing Instagram and WhatsApp.

But the jury is still out on the question of whether the massive technology companies reduce consumer welfare. They offer a wealth of digital products, such as searches, email, and social networking accounts, and consumers seem to value these products highly, even as they pay a price by giving up their privacy and allowing advertisers to target them. Moreover, almost every

abuse these platforms are accused of perpetrating can be simultaneously defended as economically efficient. Amazon, for instance, has shuttered mom-and-pop retail stores and gutted not just main streets but also big-box retailers. But the company is at the same time providing a service that many consumers find invaluable. (Imagine what it would be like if people had to rely on in-person retail during the pandemic.) As for the allegation that the platforms purchase startups to forestall competition, it is hard to know whether a young company would have become the next Apple or Google had it remained independent, or if it would have failed without the infusion of capital and management expertise it received from its new owners. Although consumers might have been better off if Instagram had stayed separate and become a viable alternative to Facebook, they would have been worse off if Instagram had failed altogether.

The economic case for reining in Big Tech is complicated. But there is a much more convincing political case. Internet platforms cause political harms that are far more alarming than any economic damage they create. Their real danger is not that they distort markets; it is that they threaten democracy.

THE INFORMATION MONOPOLISTS

Since 2016, Americans have woken up to the power of technology companies to shape information. These platforms have allowed hoaxers to peddle fake news and extremists to push conspiracy theories. They have created “filter bubbles,” an environment in which, because of how their algorithms work, users are exposed only to information that confirms their preexisting beliefs. And they can amplify or bury particular voices, thus having a disturbing influence on democratic political debate. The ultimate fear is that the platforms have amassed so much power that they could sway an election, either deliberately or unwittingly.

Critics have responded to these concerns by demanding that the platforms assume greater responsibility for the content they broadcast. They called for Twitter to suppress or fact-check President Donald Trump's misleading tweets. They lambasted Facebook for stating that it would not moderate political content. Many would like to see Internet platforms behave like media companies, curating their political content and holding public officials accountable.

But pressuring large platforms to perform that function—and hoping they will do it with the public interest in mind—is not a long-term solution. This approach sidesteps the problem of their underlying power, and any real solution must limit that power. Today, it is largely conservatives who complain about Internet platforms' political bias. They assume, with some justification, that the people who run today's platforms—Jeff Bezos of Amazon, Mark Zuckerberg of Facebook, Sundar Pichai of Google, and Jack Dorsey of Twitter—tend to be socially progressive, even as they are driven primarily by commercial self-interest.

This assumption may not hold up in the longer run. Suppose that one of these giants were taken over by a conservative billionaire. Rupert Murdoch's control over Fox News and *The Wall Street Journal* already gives him far-reaching political clout, but at least the effects of that control are plain to see: you know when you are reading a *Wall Street Journal* editorial or watching Fox News. But if Murdoch were to control Facebook or Google, he could subtly alter ranking or search algorithms to shape what users see and read, potentially affecting their political views without their awareness or consent. And the platforms' dominance makes their influence hard to escape. If you are a liberal, you can simply watch MSNBC instead of Fox; under a Murdoch-controlled Facebook, you may not have a similar choice if

you want to share news stories or coordinate political activity with your friends.

Consider also that the platforms—Amazon, Facebook, and Google, in particular—possess information about individuals' lives that prior monopolists never had. They know who people's friends and family are, about people's incomes and possessions, and many of the most intimate details of their lives. What if the executive of a platform with corrupt intentions were to exploit embarrassing information to force the hand of a public official? Alternatively, imagine a misuse of private information in conjunction with the powers of the government—say, Facebook teaming up with a politicized Justice Department.

Digital platforms' concentrated economic and political power is like a loaded weapon sitting on a table. At the moment, the people sitting on the other side of the table likely won't pick up the gun and pull the trigger. The question for U.S. democracy, however, is whether it is safe to leave the gun there, where another person with worse intentions could come along and pick it up. No liberal democracy is content to entrust concentrated political power to individuals based on assumptions about their good intentions. That is why the United States places checks and balances on that power.

CRACKING DOWN

The most obvious method of checking that power is government regulation. That is the approach followed in Europe, with Germany, for example, passing a law that criminalizes the propagation of fake news. Although regulation may still be possible in some democracies with a high degree of social consensus, it is unlikely to work in a country as polarized as the United States. Back in the heyday of broadcast television, the Federal Communications Commission's fairness doctrine required networks to

maintain “balanced” coverage of political issues. Republicans relentlessly attacked the doctrine, claiming the networks were biased against conservatives, and the Federal Communications Commission rescinded it in 1987. So imagine a public regulator trying to decide whether to block a presidential tweet today. Whatever the decision, it would be massively controversial.

Another approach to checking Internet platforms’ power is to promote greater competition. If there were a multiplicity of platforms, none would have the dominance enjoyed by Facebook and Google today. The problem, however, is that neither the United States nor the EU could likely break up Facebook or Google the way that Standard Oil and AT&T were broken up. Today’s technology companies would fiercely resist such an attempt, and even if they eventually lost, the process of breaking them up would take years, if not decades, to complete. Perhaps more important, it is not clear that breaking up Facebook, for example, would solve the underlying problem. There is a very good chance that a baby Facebook created by such a breakup would quickly grow to replace the parent. Even AT&T regained its dominance after being broken up in the 1980s. Social media’s rapid scalability would make that happen even faster.

In view of the dim prospects of a breakup, many observers have turned to “data portability” to introduce competition into the platform market. Just as the government requires phone companies to allow users to take their phone numbers with them when they change networks, it could mandate that users have the right to take the data they have surrendered from one platform to another. The General Data Protection Regulation (GDPR), the powerful EU privacy law that went into effect in 2018, has adopted this very approach, mandating a standardized, machine-readable format for the transfer of personal data.

Data portability faces a number of obstacles, however. Chief among them is the difficulty of moving many kinds of data. Although it is easy enough to transfer some basic data—such as one’s name, address, credit card information, and email address—it would be far harder to transfer all of a user’s metadata. Metadata includes likes, clicks, orders, searches, and so on. It is precisely these types of data that are valuable in targeted advertising. Not only is the ownership of this information unclear; the information itself is also heterogeneous and platform-specific. How exactly, for example, could a record of past Google searches be transferred to a new Facebook-like platform?

An alternative method of curbing platforms’ power relies on privacy law. Under this approach, regulations would limit the degree to which a technology company could use consumer data generated in one sector to improve its position in another, protecting both privacy and competition. The GDPR, for example, requires that consumer data be used only for the purpose for which the information was originally obtained, unless the consumer gives explicit permission otherwise. Such rules are designed to address one of the most potent sources of platform power: the more data a platform has, the easier it is to generate more revenue and even more data.

But relying on privacy law to prevent large platforms from entering new markets presents its own problems. As in the case of data portability, it is not clear whether rules such as the GDPR apply only to data that the consumer voluntarily gave to the platform or also to metadata. And even if successful, privacy initiatives would likely reduce only the personalization of news for each individual, not the concentration of editorial power. More broadly, such laws would close the door on a horse that has long since left the barn. The technology giants have already amassed vast quantities of customer data. As the new Department of Justice lawsuit indicates, Google’s

business model relies on gathering data generated by its different products—Gmail, Google Chrome, Google Maps, and its search engine—which combine to reveal unprecedented information on each user. Facebook has also collected extensive data about its users, in part by allegedly obtaining some data on users when they were browsing other sites. If privacy laws prevented new competitors from amassing and using similar data sets, they would run the risk of simply locking in the advantages of these first movers.

THE MIDDLEWARE SOLUTION

If regulation, breakup, data portability, and privacy law all fall short, then what remains to be done about concentrated platform power? One of the most promising solutions has received little attention: middleware.

Middleware is generally defined as software that rides on top of an existing platform and can modify the presentation of underlying data. Added to current technology platforms' services, middleware could allow users to choose how information is curated and filtered for them. Users would select middleware services that would determine the importance and veracity of political content, and the platforms would use those determinations to curate what those users saw. In other words, a competitive layer of new companies with transparent algorithms would step in and take over the editorial gateway functions currently filled by dominant technology platforms whose algorithms are opaque.

Middleware products can be offered through a variety of approaches. One particularly effective approach would be for users to access the middleware via a technology platform such as Apple or Twitter. Consider news articles on users' news feeds or popular tweets by political figures. In the background of Apple or Twitter, a middleware service could add labels such as "misleading," "unverified," and "lacks context." When users logged on to Apple and Twitter, they would see these labels on the news articles and

tweets. A more interventionist middleware could also influence the rankings for certain feeds, such as Amazon product lists, Facebook advertisements, Google search results, or YouTube video recommendations. For example, consumers could select middleware providers that adjusted their Amazon search results to prioritize products made domestically, eco-friendly products, or lower-priced goods. Middleware could even prevent a user from viewing certain content or block specific information sources or manufacturers altogether.

Each middleware provider would be required to be transparent in its offerings and technical features, so that users could make an informed choice. Providers of middleware would include both companies pursuing improvements to feeds and nonprofits seeking to advance civic values. A journalism school might offer middleware that favored superior reporting and suppressed unverified stories, or a county school board might offer middleware that prioritized local issues. By mediating the relationship between users and the platforms, middleware could cater to individual consumers' preferences while providing significant resistance to dominant players' unilateral actions.

Many details would have to be worked out. The first question is how much curation power to transfer to the new companies. At one extreme, middleware providers could completely transform the information presented by the underlying platform to the user, with the platform serving as little more than a neutral pipe. Under this model, middleware alone would determine the substance and priority of Amazon or Google searches, with those platforms merely offering access to their servers. At the other extreme, the platform could continue to curate and rank the content entirely with its own algorithms, and the middleware would serve only as a supplemental filter. Under this model, for example, a Facebook or Twitter interface would

remain largely unchanged. Middleware would just fact-check or label content without assigning importance to content or providing more fine-tuned recommendations.

The best approach probably lies somewhere in between. Handing middleware companies too much power could mean the underlying technology platforms would lose their direct connection to the consumer. With their business models undermined, the technology companies would fight back. On the other hand, handing middleware companies too little control would fail to curb the platforms' power to curate and disseminate content. But regardless of where exactly the line were drawn, government intervention would be necessary. Congress would likely have to pass a law requiring platforms to use open and uniform application programming interfaces, or APIs, which would allow middleware companies to work seamlessly with different technology platforms. Congress would also have to carefully regulate the middleware providers themselves, so that they met clear minimum standards of reliability, transparency, and consistency.

A second issue involves finding a business model that would incentivize a competitive layer of new companies to emerge. The most logical approach would be for the dominant platforms and the third-party providers of middleware to strike revenue-sharing agreements. When someone made a Google search or visited a Facebook page, the advertising revenue from the visit would be shared between the platform and the middleware provider. These agreements would likely have to be overseen by the government, since even if the dominant platforms are eager to share the burden of filtering content, they should be expected to resist sharing advertising revenue.

Yet another detail to be worked out is some sort of technical framework that would encourage a diversity of middleware products to spring forth. The

framework would need to be simple enough to attract as many entrants as possible, but sophisticated enough to fit atop the big platforms, each of which has its own special architecture. Moreover, it would have to allow middleware to assess at least three different kinds of content: widely accessible public content (such as news stories, press releases, and tweets from public figures), user-generated content (such as YouTube videos and public tweets from private individuals), and private content (such as WhatsApp messages and Facebook posts).

Skeptics might argue that the middleware approach would fragment the Internet and reinforce filter bubbles. Although universities might require their students to use middleware products that directed them to credible sources of information, conspiracy-minded groups might do the opposite. Custom-tailored algorithms might only further splinter the American polity, encouraging people to find voices that echo their views, sources that confirm their beliefs, and political leaders that amplify their fears.

Perhaps some of these problems could be resolved with regulations that required middleware to meet minimum standards. But it is also important to note that such splintering can already happen, and it may well be technologically impossible to prevent it from occurring in the future. Consider the path taken by followers of QAnon, an elaborate far-right conspiracy theory that posits the existence of a global pedophilia cabal. After having their content restricted by Facebook and Twitter, QAnon supporters abandoned the big platforms and migrated to 4chan, a more permissive message board. When 4chan's moderation teams started tempering incendiary comments, QAnon followers moved to a new platform, 8chan (now called 8kun). These conspiracy theorists can still communicate with one another through ordinary email or on encrypted

channels such as Signal, Telegram, and WhatsApp. Such speech, however problematic, is protected by the First Amendment.

What's more, extremist groups endanger democracy primarily when they leave the periphery of the Internet and enter the mainstream. This happens when their voices are either picked up by the media or amplified by a platform. Unlike 8chan, a dominant platform can influence a broad swath of the population, against those people's will and without their knowledge. More broadly, even if middleware encouraged splintering, that danger pales in comparison to the one posed by concentrated platform power. The biggest long-term threat to democracy is not the splintering of opinion but the unaccountable power wielded by giant technology companies.

GIVING BACK CONTROL

The public should be alarmed by the growth and power of dominant Internet platforms, and there is good reason why policymakers are turning to antitrust law as a remedy. But that is only one of several possible responses to the problem of concentrated private economic and political power.

Now, governments are launching antitrust actions against Big Tech platforms in both the United States and Europe, and the resulting cases are likely to be litigated for years to come. But this approach is not necessarily the best way to deal with platform power's serious political threat to democracy. The First Amendment envisioned a marketplace of ideas where competition, rather than regulation, protected public discourse. Yet in a world where large platforms amplify, suppress, and target political messaging, that marketplace breaks down.

Middleware can address this problem. It can take that power away from technology platforms and hand it not to a single government regulator but

to a new group of competitive firms that would allow users to tailor their online experiences. This approach would not prevent hate speech or conspiracy theories from circulating, but it would limit their scope in a way that better aligned with the original intent of the First Amendment. Today, the content that the platforms offer is determined by murky algorithms generated by artificial intelligence programs. With middleware, platform users would be handed the controls. They—not some invisible artificial intelligence program—would determine what they saw.

Copyright © 2022 by the Council on Foreign Relations, Inc.

All rights reserved. To request permission to distribute or reprint this article, please visit ForeignAffairs.com/Permissions.

Source URL: <https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology>