Stanford | Program on Democracy and the Internet
Cyber Policy Center

Stanford PACS
Center on Philanthropy and Civil Society

REPORT OF THE WORKING GROUP ON PLATFORM SCALE

STANFORD UNIVERSITY

Francis Fukuyama, Barak Richman, Ashish Goel
Roberta R. Katz, A. Douglas Melamed,
Marietje Schaake

I. INTRODUCTION

The internet economy has produced digital platforms of enormous economic and social significance. These platforms—specifically, Google, Facebook, Amazon, Twitter, and Apple—now play central roles in how millions of Americans obtain information, spend their money, communicate with fellow citizens, and earn their livelihoods. Their reach is also felt globally, extending to many countries around the world. They have amassed the economic, social, and political influence that very few private entities have ever obtained previously. Accordingly, they demand careful consideration from American policymakers, who should soberly assess whether the nation's current laws and regulatory institutions are adequately equipped to protect Americans against potential abuses by platform companies.

The Program on Democracy and the Internet at Stanford University convened a working group in January 2020 to consider the scale, scope, and power exhibited by the digital platforms, study the potential harms they cause, and, if appropriate, recommend remedial policies. The group included a diverse and interdisciplinary group of scholars, some of whom had spent many years dealing with antitrust and technology issues.

A number of other groups and organizations have addressed concerns about digital platform dominance in recent years, including the Stigler Center at the University of Chicago, the Thurmond Arnold Project at Yale, the Berkman Klein Center at Harvard, the Shorenstein Center at the Harvard Kennedy School, the Open Markets Institute, and Germany's "Competition Law 4.0" Commission. Most of these groups focused on issues of monopoly power within the framework of existing US antitrust and European competition law, asking whether and how the platforms might have violated those laws, offering potential remedies, and, in some cases, suggesting modifications of current law to deal with specific characteristics of digital services. The European Commission has also conducted numerous antitrust investigations of digital platforms and is in the process of updating EU competition regulation. In the US, several Congressional committees have been investigating the platforms for potential antitrust violations, as has a group of state attorneys-general, and the Department of Justice recently filed an antitrust suit against Google.

"The potential harms to society from the dominant platforms are not solely economic."

Our Working Group determined early on that we did not wish to duplicate the prior analyses of how existing (or modified) antitrust laws might apply to the digital platforms, though we refer to and elaborate on such analyses in our discussions of harms and remedies below. Antitrust laws address harm to competition that results from anticompetitive conduct, essentially focusing on abuses of economic power, but the potential harms to society from

the dominant platforms are not solely economic. The scale and concentrated power of the platforms also cause *social harms*, including loss of privacy and monopolization and manipulation of attention, and *political harms*, including threats to democratic discourse and deliberation and, ultimately, to democratic choice in the electoral process.

In our discussions with various stakeholders, we found that, for many people, the most significant fears surrounding platform scale centered around potential political harms. Since 2016 there has been substantial discussion about fake news, filter bubbles, targeted political advertising, propagation of conspiracy theories, and the power of platforms to vastly amplify (or bury) particular voices in democratic political debate. The ultimate fear is that the platforms have amassed sufficient power that they could potentially sway an election, either as a matter of deliberate choice or as a result of being unwittingly manipulated by other political actors. These political harms have not yet been given sufficient attention in policy circles, especially with respect to possible remedies, so we discuss those harms and potential remedies at considerable length in this report.

"The scale of today's platforms gives them extraordinary power to reach broad audiences."

In this regard, scale matters acutely. We expect democratic debate and politics to be pluralistic and to protect freedom of speech. But the scale of today's platforms gives them extraordinary power to reach broad audiences, much like the network television oligopoly of the 1950s and '60s, and their control over what appears and is disseminated on their platforms can shape both beliefs and behavior.

We can illustrate the nature of these concerns with a recent example. In late May 2020, Twitter for the first time applied warning labels to two of President Trump's tweets, one of which falsely claimed that mail-in balloting would lead to widespread voter fraud.[1] Trump accused the platform of censorship, and a few days later issued an executive order directing all executive departments and agencies to review Section 230 of the 1996 Communications Decency Act, which shields the digital platforms from private liability for the materials they carry. The order asserted "Free speech is the bedrock of American democracy," and that "we cannot allow a limited number of online platforms to hand pick the speech that Americans may access and convey on the internet."[2]

President Trump's critics were quick to point out that the First Amendment actually protects speech by private companies like Twitter and constrains only the government.[3] There was also an extended debate over the administration's ability to unilaterally alter the interpretation of Section 230, and what the effects of lifting this protection would actually be.

What was missing from the subsequent discussion was a recognition that the dominant platforms do, in fact, control an enormous amount of the nation's political communication. Twitter is not just one of many digital platforms in a competitive market for online information: it has grown to a size—and it individually enjoys sufficient power—where it can significantly shape the way Americans think about politics. Facebook and Google are substantially larger platforms with arguably even more power. In the 1960s, when three huge networks dominated broadcast media, the federal government sought to regulate the kinds of speech they could carry under what was known as the Fairness Doctrine, a power that, because of what were perceived as unique technological constraints on the entry of new rivals, was held by the Supreme Court to be consistent with the First Amendment. The court made this finding on the basis of the networks' dominance of the limited broadcast spectrum available at that time. The internet's "spectrum" is obviously not limited in the same way, but network economies appear to give Twitter, Google, and Facebook a comparable degree of power today.

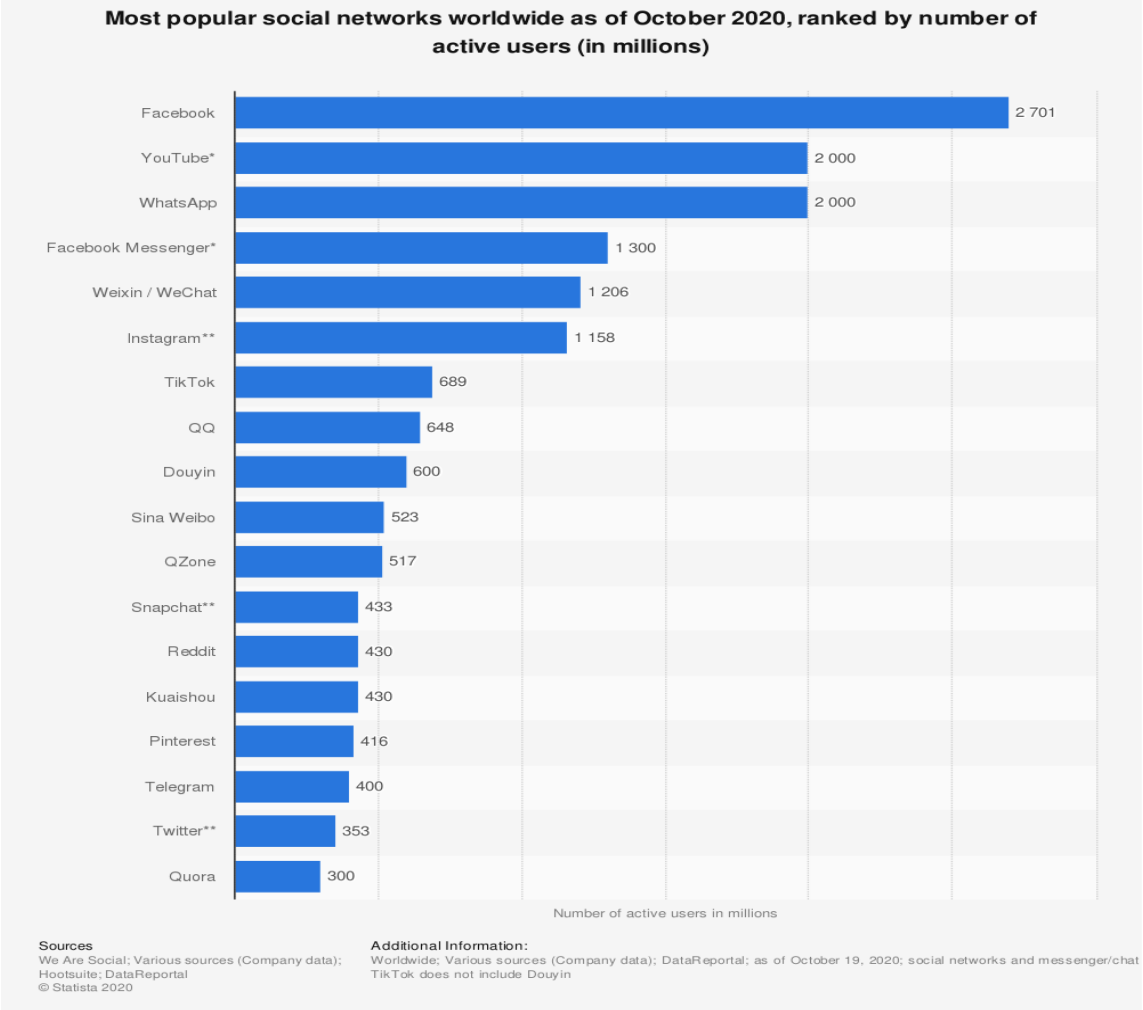


Figure 1: *Major platforms by number of active users.*

It is sometimes asserted that Facebook has become the new "public square."[*] To the extent that this is true, we should note that this role has not been legitimated by any act of democratic choice. The square is run by business executives, for profit. European public broadcasters like the BBC or ZDF that perform a similar function have been legislatively approved, and are governed by a host of institutional rules that seek to ensure that they serve public interest and enjoy editorial independence. Obviously, Facebook, a company largely controlled by a single private individual, has no similar legitimacy or independent oversight, nor does it adhere to publicly chosen editorial standards.

"Pressuring the platforms to curate political content in the manner of a media company is not a long-term solution to the problem they pose for democracy."

Many of President Trump's critics believe that Twitter has not gone far enough in suppressing or fact-checking the President's tweets, or those of his followers. They lambasted Mark Zuckerberg for stating that Facebook would not follow Twitter's lead and try to moderate political content. Many would like to see the internet platforms behave like media companies in curating the political content of what they carry and to hold public officials accountable. But in our view, today's large internet platforms exist in a far less competitive environment than legacy media companies; pressuring them to curate political content in the manner of a media company is not a long-term solution to the problem they pose for democracy. There can be no assurance that large digital platforms will use their power for benign purposes. Experience with broadcast media like Fox and Sinclair, and arguably other media outlets as well, suggests the contrary.[4]

[*] In Packingham v. North Carolina 137 S. Ct. 1730 (2017), Supreme Court characterized the internet, with particular emphasis on social media sites such as Facebook, as the "modern public square."

Figure 2: *President Trump's October 2020 tweet about mail-in ballots was labeled by Twitter as possibly misleading.*

The essential problem is that the digital platforms have enormous control over the information flows that shape political discourse. That power could be misused by manipulative third parties or by the platforms themselves. Asking or hoping that the platforms will use their influence to counteract abuses of public power sidesteps the problem of their own underlying power. The solution must be to limit the power of the platforms with the aim of ensuring democratic values, pluralism, transparency, and accountability.

There are numerous strands of modern democratic theory that uphold the idea that political institutions need to check and limit arbitrary power regardless of the identity of the power holder. It is implicit in John Rawls' concept of the "veil of ignorance," in which fair rules in a liberal society must be drawn up without regard to knowledge of the person or persons to whom they apply. The 1780 Constitution of the State of Massachusetts, drafted by John Adams, Samuel Adams, and James Bowdoin, stated that "the executive shall never exercise the legislative [or] judicial powers… to the end it may be a government of laws and not of men."[5] James Madison's famous Federalist No. 51 lays the ground for a system of divided powers by arguing that in "framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[6] The only practical solution to this problem was to comprehend "in the society so many separate descriptions of citizens as will render an unjust combination of a majority of the whole very improbable, if not

impracticable." In other words, power could be controlled only by dividing it, in a system of checks and balances.

> "Private power faces no checks like popular elections; it can be controlled only by the government (through regulation) or by competition among power holders."

These strictures were applied by their authors to state power, but they would apply doubly to concentrations of private power. Private power faces no checks like popular elections; it can be controlled only by the government (through regulation) or by competition among power holders. American suspicion of concentrated power has always meant that the country has favored market competition as the preferred means of controlling and limiting private power. Fear of the economic and political consequences of monopoly power was among the concerns that motivated passage of the Sherman, Clayton, and FTC Acts, as fears of concentrated political power and economic power go hand in hand.

This is a danger that transcends current political divides. Today, many conservatives who complain about political bias on the internet platforms suspect that the people who run the platforms—Jack Dorsey, Mark Zuckerberg, Sundar Pichai, or Jeff Bezos—tend to be socially progressive, and that those political beliefs influence the content curation policies of the platforms, even as they are driven in large part by commercial self-interest. Some progressives raise similar concerns about bias, though bias from the opposite end of the political spectrum. Regardless of political leaning, the issue comes down to power and transparency, which can be illustrated by imagining if Google or Facebook were run by Rupert Murdoch, Charles Koch, Jack Ma, or Julian Sinclair Smith. Murdoch's control over Fox News and the *Wall Street Journal* already gives him enormous political clout, but at least the effects of that control are plainly visible to everyone. If he were to control Facebook or Google, he could subtly alter ranking or search algorithms that would strongly affect people's political views, but in a far less transparent manner. Today, if you are a liberal, you can simply watch CNBC instead of Fox; under a Murdoch-controlled Facebook, you may not have a similar choice if you want to share news stories or mobilize political activity with your friends.

> "The platforms know what we buy, where we work, where we live, where we go, with whom we communicate, and what we value. They know our friends and family, our income and our possessions, and many of the most intimate details of our lives."

Consider also that the platforms—Facebook, Amazon, and Google in particular—possess information about our individual lives that empower them to engage in pernicious conduct that prior monopolists never had. They know what we buy, where we work, where we live, where we go, with whom we communicate, and what we value. They know our friends and family, our income and our possessions, and many of the most intimate details of our lives. What if a platform executive 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, perhaps if Facebook were to team up with a politicized Department of Justice. How can we ensure that the platforms' amassing of personal information will not corrupt government powers and the political process?

The platforms' ability to gather information and curate content would not be as problematic if they were less dominant in their role as information filters—if, for example, there were a large number of important digital intermediaries for news and other information providers. In a more competitive platform environment, such curation would be much less of an issue. Indeed, curation would be highly desirable in the aggregate, since a totally uncurated internet quickly becomes a miasma of disinformation, spam, pornography, and incivility.

The growing political power exercised by the digital platforms is like a loaded weapon sitting on the table in front of us.[†] At the moment, we are reasonably confident that the people sitting on the other side won't deliberately pick up the gun and shoot us with it. The question for American democracy, however, is whether it is safe to leave the gun on the table, where another person with less good intentions—whether the owners of the platforms or outsiders who figure out how to manipulate them for their purposes—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 or on the merits of their business models, which is why we place checks and balances on that power.

"We do not believe the antitrust laws in their current form provide adequate remedies for non-economic harms."

While some have suggested that the antitrust laws may be sufficient to address these kinds of political harms, in addition to the economic harms, for reasons we discuss in detail in Part IV

[†] On the danger of failing to address shortcomings in the law, it is useful to remind ourselves of Justice Robert Jackson's dissent in Korematsu v. United States, 323 U.S. 214 (1944). After the Supreme Court deemed the internment of Japanese Americans during World War II to be constitutional, Justice Jackson warned that, "the Court for all time has validated the principle of racial discrimination in criminal procedure and of transplanting American citizens. The principle then lies about *like a loaded weapon* ready for the hand of any authority that can bring forward a plausible claim of an urgent need." 323 U.S. at 246 (emphasis added).

of this report, we do not believe the antitrust laws in their current form provide adequate remedies for non-economic harms. Although having a multiplicity of non-dominant platforms could address such harms, neither the US nor the EU is likely to break up Google or Facebook in the way that Standard Oil or AT&T were broken up in the 1900s. These platform companies would of course fiercely resist such an attempt, and even if they eventually lost, the breakup process would take years if not decades to accomplish. Moreover, it is not clear that breaking up Facebook would solve the underlying problem; social media's rapid scalability (an attribute of digital platforms that we discuss in Section II of this report) could allow a baby Facebook to quickly grow back into the dominance previously enjoyed by its parent.

Updates to antitrust laws to reflect the specifics of digital platforms are anticipated in the EU and perhaps in the US. These updates could clarify how antitrust applies to the new technologically driven businesses and potentially reduce or inhibit the power of the platforms, which in turn could potentially ameliorate some of the broader concerns about speech, democratic process, and equality. But in the absence of such updates, it is important to consider a wider range of possible regulatory policy responses.

"A combination of regulation and new technology might enable new forms of competition to emerge on top of the existing platforms, an approach we call a 'middleware' solution."

Government regulation has long been used to deal with problems posed by natural monopolies like public utilities, and similar regulation could be applied to the internet platforms as well. Privacy law might be employed to forbid platforms from using data generated in one field of activity to give themselves an advantage in another, unrelated domain. Europe's General Data Protection Regulation (GDPR) already provides these protections, at least in theory. And a combination of regulation and new technology might enable new forms of competition to emerge on top of the existing platforms, an approach we call a "middleware" solution that we explore below. This technological intervention has the potential to restore certain forms of competition and to address societal harms without resorting to traditional antitrust remedies.

The following pages of this report are organized into three sections. In Section II, we describe in summary form the key features of the digital platforms that pose the current policy challenges. In Section III we describe in more detail the nature of the economic, social, and political harms we have referenced in this Introduction. And in Section IV, we examine various policy interventions, with emphasis on remedies for political harms, including, most particularly, the possibilities of the middleware intervention.

II. Key Features of Digital Platform Dominance

Six key features of digital markets should shape policy strategies. These features demonstrate how the platforms' economic dominance is intertwined with their influence over social and political activities. They suggest that market forces alone are unlikely to mitigate their dominance in the foreseeable future, that their activities implicate concerns that lie outside the traditional domain of economic regulation, and that their dominance is unlike that seen before from even dominant media empires. In summary, these features, which we further discuss in Part III below as they pertain to associated economic, social, and political harms, are the following:

1. *Emphasis on Dynamic Competition*. There has been broad recognition that the combination of high fixed costs and close to zero marginal costs, together with network externalities, makes competition in the digital world different from most pre-digital markets. As several existing reports and the *US v. Microsoft* (2001) antitrust case have indicated, there is often less competition for market share than there is competition for the entire market, and these features have significant implications for economic policy.[7] In a dynamic setting, that means that the principal source of competition involves the entry of new rivals and the innovations they offer.

"The centrality of accumulating personal data across multiple domains introduces new economic challenges and poses unique risks to personal privacy."

2. *Data as a Key Asset*. Most digital markets are driven by the possession and analysis of large volumes of consumer data. Incumbents with larger data resources enjoy competitive advantages over rivals, and incumbents with greater access to inflows of consumer data may be able to maintain a sustained competitive advantage over future entrants. Many dominant platforms obtain their market leadership by offering consumers services in exchange for their agreement to share data, though such user agreements are frequently complicated and rarely understood. The centrality of accumulating personal data across multiple domains introduces new economic challenges and poses unique risks to personal privacy.

3. *Intermediating Networks*. Digital platforms serve as intermediaries for both social and business networks. Increasingly, our social, economic, and political activities rely on these intermediating networks. They play major roles in facilitating our personal interactions, business transactions, and collective mobilization, and changes to their algorithms would influence how individuals and businesses interact.

“Our economic and political ecosystems are shaped under the direction of the platforms’ particular interests, which are often expressed behind an algorithmic veil.”

4. *The Opacity of Platform Interventions*. Unlike prior connective technologies, such as newspapers, electrical wires, or telephone lines, digital platforms can introduce filters to our connections that are hard to detect. Many dominant digital platforms utilize algorithms that determine how connections are facilitated and information is shared, and these algorithms often change, sometimes instantaneously under the direction of artificial intelligence, in accordance with the platforms’ private objectives. Our economic and political ecosystems are shaped under the direction of the platforms’ particular interests, which are often expressed behind an algorithmic veil. The centrality of these platforms makes us dependent on their interventions, and the automation and opacity of their operations complicate any effort to monitor their conduct.

5. *Size and Scale*. The global dominance enjoyed by the biggest digital firms represents an enormous amount of economic power. Even though law, including antitrust law, advances generalized rules that apply to all sectors, policy towards the digital platforms needs to recognize that rules and regulations in this sector have disproportionate economic and social consequences. Moreover, the platforms’ dominance tends to reinforce itself. Scale economies advantage dominant platforms over smaller platforms, and scale economies that enable the acquisition of consumer and market data generate scope economies that allow dominant platforms to extend their dominance into adjacent businesses.

6. *Economic Concentration and Market Power*. The paucity of dominant platforms allows each one to exercise market power as an intermediary and reduces citizens’ outside options for alternatives. The dominance of a platform enhances its ability to harm potential competitors, including trading partners, civic groups, and political voices, by disfavoring access to the platform, denying access altogether, or enabling third parties with access to manipulate information flows. Redressing the platforms’ market power as intermediaries might necessitate developing viable market alternatives.

III. Digital Platform Harms

It deserves emphasis that digital platforms, and in particular the dominant platform companies, provide many services that individuals across the world value highly, and that they provide enormous benefits to the world in many ways. A recent study indicates that

individuals would demand substantial payments to forgo services that digital platforms provide for free.[8]

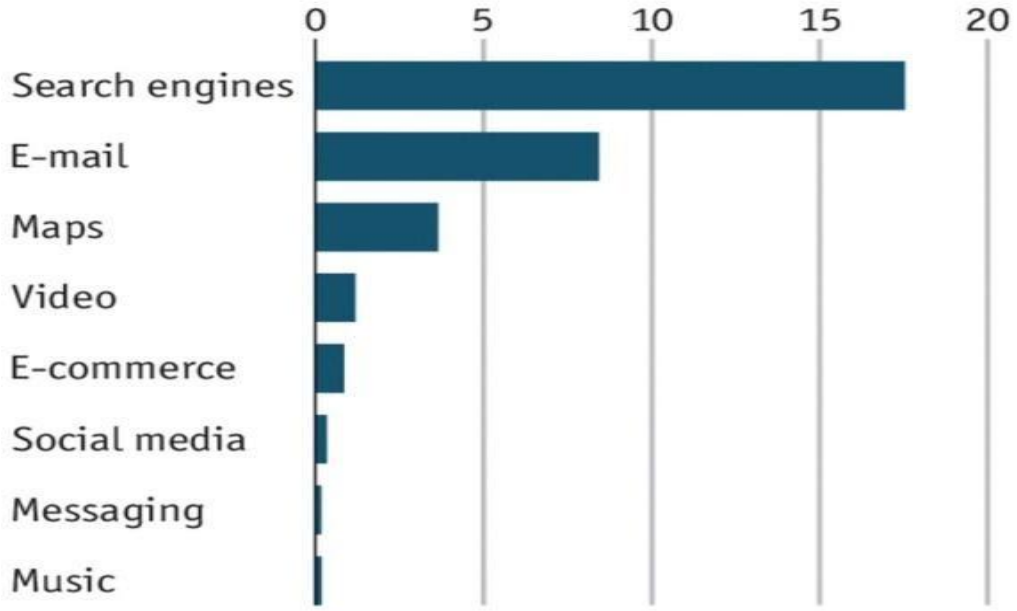


Figure 3: *Median payment accepted to forgo the use of internet service for a year, $'000*[9]

In addition, the dominant digital platforms facilitate speech and the dissemination of ideas, including by those who do not control powerful government or private entities. They thereby have contributed meaningfully not just to economic growth and productivity but to the advancement of democratic values. Twitter, for example, was instrumental in facilitating pro-democracy movements during the Arab Spring and in Ukraine's Revolution of Dignity, and platform engagement appears associated with certain forms of political participation. [10]

However, dominant platforms also cause economic harm, threaten privacy interests, and distort our social and political networks in unconventional ways. They are at the heart of what is considered surveillance capitalism. Indeed, while they have contributed to democratizing social movements, they have also been instrumental in facilitating the surveillance of those same movements, to the detriment of the human rights of its activists. Crafting policy responses requires understanding and articulating these harms in detail.

A. Economic Harms

As is detailed in the Stigler Center report and elsewhere, dominant digital platforms can impose significant economic harms.[11] We highlight certain economic harms that demand policy attention, whether from the antitrust laws or from other legal remedies.

Entry barriers

A hallmark economic danger from digital monopolists with scale efficiencies is that their pursuit of short-term, economically defensible activities might nonetheless impede dynamic innovation and thereby have anticompetitive consequences. Statically efficient measures by incumbents might, for example, leave little room for competing entrants and thus offer inadequate opportunity for their innovations to reach efficient scale. Although this phenomenon is not a new problem, the problems presented by dominant platforms might be much more serious in degree and could warrant policy interventions that would stimulate dynamic competition. Allowing platform dominance to persist, even if the platforms are engaging in value-enhancing conduct, might lead to an entrenchment of dominance that limits innovative entry.

Exclusionary conduct

Dominant business entities are able to engage in anticompetitive conduct, including restrictive agreements with third parties, predatory trading practices, agreements that restrict potential rivals, and acquisitions of nascent competitors, that can entrench their dominance and stifle competitive threats. This is the kind of conduct that is targeted by the antitrust laws.

Platform monopolies can also harm competitors and consumers in the absence of clearly anticompetitive conduct. The platforms' enormous scale means that changes in business practices—altering an algorithm, say—have significant ramifications for businesses in ancillary markets. Though these platform practices might have strong business justifications, they may also harm competitors, stifle competition, or foreclose socially fruitful innovation. In such cases, even facially defensible practices could harm consumer and total welfare.

Dominant platforms can also reduce the threat of new competition by acquiring potential rivals and other smaller companies. Consider the list of Alphabet startup purchases.[12] Some of these acquisitions likely enabled the creation of products and capabilities that otherwise would never have been developed. Some acquisitions might have targeted potential competitors that would have flourished and changed market dynamics absent the acquisitions. And some created valuable products, but at the expense of eliminating the gains that would have resulted if the acquired firms had remained independent of Alphabet's control and contributed to important innovations that would not have been in Alphabet's interest. Although it is never possible to know for sure what would happen to these companies absent their acquisition by Alphabet, policymakers might nonetheless need to scrutinize similar acquisitions to determine whether blocking them or requiring some other remedy would be likely to enhance competition and consumer welfare.

Extending market power into new, often vertically linked markets

Many dominant digital companies employ business models that invite other companies to offer goods and services off their platforms. For example, independent companies market

their products on the Amazon site, rely on Google's search engine to attract customers, and sell apps through Apple's App Store. At the same time, these digital platforms offer their own competing services and products, making them at once a supplier and a rival to these independent sellers. The ability of platforms to provide their own products and services could enable the realization of important synergies of scale and scope economies that increase product quality, reduce costs, and enhance economic welfare. But there is also a danger that dominant digital platforms will disfavor rival suppliers that might be more efficient or innovative in their adjacent businesses, especially those that might also be able to evolve into significant competitors of the platforms themselves. That kind of self-preferencing by the platforms could reduce economic welfare and perpetuate the dominance of the platforms.

Economic power facilitates political power that might be used to suppress competition
Finally, entrenched economic dominance also imposes harms to our system of governance. Large corporations have always utilized their economic resources to generate policies they find favorable, and the Sherman Act was motivated, in part, because of how trusts in the Gilded Age purchased favors from state legislatures.[13] Thomas Philippon argues that the increasing concentration we have seen in a wide variety of sectors is due to the ability of large companies to protect themselves politically.[14] The economic size of today's dominant platforms might give them especially potent power to exert lobbying, harness political resources, and employ other heft to prevent competition. Their influence on shaping public opinion and their role in disseminating information suggest they could advocate for themselves in policymaking arenas in ways that industrial monopolists cannot.

Economic power can also be translated into political power beyond that used to promote the economic interests of the platforms themselves, as we discuss in the section on Political Harms below.

B. Social Harms: Loss of Privacy

The loss of privacy can have widespread deleterious effects on both individuals and societies, and such social harms are taken seriously by many people. In Europe, privacy is a fundamental right, not a matter of consumer choice, and the right to privacy is written into the national laws of most EU member states and into the EU's founding treaties.[15] Privacy rules like the GDPR are therefore not contingent on strong popular support, even though support is strong. In the US, there is no such legal imperative, and privacy protections are only supplied by ordinary laws, like the California Consumer Privacy Act of 2018 (enacted in 2020), which are subject to political demands.

"Although there might be value creation behind accumulating so much personal data, including through targeted advertising, market research, and product development, its accumulation raises unique risks to personal privacy that warrant regulation."

The large internet platforms have given consumers products that they obviously value, and many products come at a zero-dollar price; consumers instead pay by providing personal data or acceding to incursions on personal privacy. Because many platform business models rest on the acquisition of personal data, dominant platforms have accumulated personal data that is remarkably comprehensive and detailed. Some platforms accumulate personal data across multiple domains, such as search preferences, website activity, and geolocation from smartphone apps. Although there might be value creation behind accumulating so much personal data, including through targeted advertising, market research, and product development, its accumulation raises unique risks to personal privacy that warrant regulation.

There is a concern that American consumers are not fully aware of the data they allow the digital platforms to accumulate. Even though consumers sign terms-of-use agreements before engaging with any of the platforms, such agreements sometimes do not adequately and cogently disclose how the platforms will use personal data. Moreover, even if the terms-of-use agreements do fully and fairly disclose the platform's data policies, it is likely that consumers do not fully comprehend the implications of their data disclosure and the degree of monitoring to which they have agreed.[‡] It is not clear whether consumers understand the magnitude of the privacy losses they incur and the ways in which their privacy has been compromised, and it is not clear if or the extent to which they would agree to incur those costs if they did.

Even if consumers fully understand and agree to detailed monitoring, there are societal concerns when individual companies control such enormously detailed personal data. Possessors of personal data could blackmail individuals engaging in embarrassing or illegal behavior. Even assuming the platforms refrain from exploiting their customers, their data could be monetized and sold to clients, hacked by bad actors, or obtained by subpoena by

[‡] For example, a 2019 Pew Research Center study found that 74% of surveyed Facebook users did not know that Facebook provides a list of their interests that informs its algorithm on the "Your ad preferences" page, and approximately half of users were uncomfortable that Facebook had this list. See Paul Hitlin and Lee Rainie, "Facebook Algorithms and Personal Data," Pew Research Center, January 16, 2019, https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.

malign politicians. The mere existence of the detailed data can pose dangers to individual liberty and other non-economic values.

> “Many of the divisive consequences of online splintering, including political polarization, voter disenfranchisement, and discrimination, are exacerbated because platforms obtain detailed personal information.”

There are also broader dangers in allowing platforms to gather users’ personal data. Many of the divisive consequences of online splintering, including political polarization, voter disenfranchisement, and discrimination, are exacerbated because platforms obtain detailed personal information. Advancing privacy protections might therefore help mitigate such harms, and giving individuals ownership rights over their data—including allowing them to take their data to another platform—might induce competing platforms to enhance privacy protections to attract users.

How Americans will respond if they acquire greater understanding of the full extent to which the large platforms have gathered data on them remains unclear, but there appears to be a growing desire for greater privacy protections, at least in areas such as health information. This may represent a change from the past, when many people appeared willing to disclose details of their personal lives in exchange for access to social media, an email account, or other digital offerings. New policies will need to respond to specific harms and reflect societal priorities, as well as reflect citizen concerns.

It should be mentioned that advancing privacy can be in tension with the desire to increase competition. For example, large companies may find it easier than small companies to meet strict privacy standards. And some steps that have been proposed to address competition concerns, such as increased data portability or network interoperability, would facilitate wider access to personal information and might thus undermine privacy interests.

In addition, privacy and transparency need to be considered in relation to each other. We desire transparency to advance our understanding of the impact of digitization and to ensure accountability, but we also want companies to protect the privacy of all users. Expanding researcher access and bringing greater transparency to platforms’ privacy policies would usefully inform policymakers’ understanding and could reveal strategies to hold platforms accountable for their privacy policies. Standardizing the treatment of data—for example, defining the levels of data and associated protections regarding data acquisitions and uses—

could also bring transparency to data markets and facilitate oversight. Policies will need to be clear about this interplay among privacy, transparency, and competition.

C. Political Harms

As we outlined in the Introduction to this report, dominant digital platforms present a number of interrelated challenges to modern political institutions that were not associated with industrial trusts. These platforms disseminate a significant share of the information that shapes our politics and economy. Their ability to constrain, magnify, or influence these informational pathways could cause significant harm to economic rivals, political foes, and democratic interests. Some of these harms are direct consequences of platform algorithms or other business practices designed to keep people online and receptive to advertisers. Some of these harms result from third parties using or manipulating the platforms and take place because the platforms are either unwilling or unable to prevent them. And some harms might be a combination of the two—harms that occur because the platforms invite and profit from certain destructive conduct by active third-party users. In general, these political harms fall into four categories.

Boosting or stifling different viewpoints
Dominant internet platforms can affect the voices we hear. Digital platforms offer access and attention to voices and businesses that would otherwise be more isolated, thereby likely increasing diversity in many markets. But one source of their success is the scale they provide users, which in turn means there are few dominant platforms. A voice or product that is boosted by a platform gains marked prominence, whereas a product or voice that is excluded from a dominant platform suffers significant harm since there are few, if any, substitutes for the platform. Sometimes even inadvertent actions have pointed consequences. When a platform changes its algorithms, it might substantially boost some voices or products while stifling or quieting others.[§]

Therefore, the policies of the dominant platforms, even those that are not intended to quiet viewpoints, can affect the national discourse. Moreover, the operationalization of these policies is hard to monitor and perhaps even hard to understand. The opacity of the underlying algorithms, many of which are automated, make identification and oversight extremely difficult. This means the platforms might, without our detection, heavily shape the voices we hear and information we see. It might also mean that the platforms are vulnerable

[§] In some cases, these actions may be intentional. For example, after concerns that a Facebook algorithm redesign to reduce the presence of political news would be more harmful for right-leaning sites, Facebook engineers altered their changes so that left-leaning sites would face more of the impact. This change was ultimately approved by CEO Mark Zuckerberg. See Deepa Seetharaman and Emily Glazer, "How Mark Zuckerberg Learned Politics," *Wall Street Journal*, October 16, 2020, https://www.wsj.com/articles/how-mark-zuckerberg-learned-politics-11602853200.

to nefarious manipulation by third parties, who might hijack platform algorithms for political ends.

Power over content dissemination
Relatedly, dominant platforms have the power, perhaps as yet untapped, to shape our politics and elections. Digital platforms sometimes act as the producers of content, not just as wires that connect a content provider with a viewer. Their dominance enables them to play a strategic role in spreading and broadcasting information, with an eye towards shaping political outcomes that could advance their commercial or political interests.

"There is a widespread sense that the ability to spread misinformation and shape civic discourse threatens the mechanisms that underlie democracy."

Virality of misinformation
The pervasiveness of the digital platforms can distort the flow of information and perhaps encourage the spread of misinformation. The dominance of individual platforms and their business model that encourages clicks mean that some social media platforms encourage virality without commensurate regard for the quality of content, foreign interference, or effects on democratic political outcomes. There is a widespread sense that the ability to spread misinformation and shape civic discourse threatens the mechanisms that underlie democracy. This might be a natural consequence of having so many citizens rely on the same algorithms to get their real-time news updates.

Undermining social cohesion
While social media platforms can offer new forms of community, they can also disintermediate society, by, for example, replacing geographically connected affinity groups like churches and clubs with dispersed groups of people connected only online by shared ideas or interests. This transition can have two deleterious effects. It can undermine some social cohesion by replacing relationships of proximity with those of cognition, and, in so doing, it can exacerbate affective sorting by which people do not associate with, and thus are less likely to understand and trust, those who have different ideas or interests. Both of these contribute to political instability.

Some, and perhaps many, of the platforms might welcome a regulatory intervention that relieves them from the pressure of policing content or otherwise serving as a guardian of democratic discourse. The current political climate has forced many platform executives to take actions in a highly polarized setting, wherein any action or inaction necessarily alienates a large group of their users. We believe the middleware remedy we propose below could

allow the companies' leaders to offload controversial decisions to a far more competitive and diverse ecosystems of firms, thus allowing the platforms instead to focus on their primary missions of serving users and meeting financial objectives.

IV. POTENTIAL POLICY RESPONSES TO HARMS

A. Enforcing Current Antitrust Laws

At present, several antitrust investigations and legal actions targeting the major platforms are underway, and more are sure to come.[16] There are good reasons why policymakers have turned to antitrust laws to offset the power of internet platforms. The Sherman Act was originally passed to curtail the growing dominance of the nineteenth century trusts, and it seems natural to invoke it to counter today's economic leviathans.

As "the Magna Carta of Free Enterprise," the Sherman Act is normally invoked to redress the economic harm from anticompetitive behavior, but some antitrust remedies might also have the effect of ameliorating the dominant platforms' political threat to democratic institutions.[**] In this section, we review some potential antitrust actions against dominant internet platforms and assess their capacity to restrain the platforms' power, with particular focus on their power to cause political harms.

Addressing alleged platform abuses
The source of the platforms' power is their control over important internet markets. If antitrust enforcement could prevent the use of that power to exclude rivals and thereby perpetuate and expand their dominance, perhaps antitrust law could also reduce the platforms' political power. A review of the most likely antitrust remedies that target the use of platform power under current antitrust law, however, suggests that such remedies may not effectively address the political harms of greatest concern, even if a Sherman Act suit is ultimately successful.

One set of antitrust causes of action would target the possible exclusionary conduct that maintains or extends the platforms' dominance. Such conduct could potentially include Amazon prohibiting its third-party sellers from selling products at a lower price on any

[**] In United States v. Topco Assocs., Inc., 405 U.S. 596 (1972), Justice Thurgood Marshall referred to antitrust law and the Sherman Act as "the Magna Carta of Free Enterprise."

competing website,[††] Apple's use of most-favored-nation agreements with publishers to secure its iBookstore,[17] or Google's use of restrictive contracts to secure its search application as the default choice on smartphones.[18] Preventing such conduct would increase the likelihood that the dominance of the platforms would be eroded by innovation and new competition over time, but it would not directly or quickly reduce the dominance of the platforms.

A related category of claims would target conduct that denies or limits a competitor's access to their dominant internet marketplaces, thereby preserving the platforms' own advantage in ancillary markets. These claims might target Apple's purported obstruction of competing app designers from selling apps on the App Store,[19] Amazon's disadvantaging rivals when they sell products that compete with Amazon,[20] and Google's structuring of search results to advantage products in which Google has a financial interest.[21] If successful, these claims might make competition more robust in adjacent markets, but they are unlikely to meaningfully reduce the power of the platforms themselves. The platforms would still exercise control over communications, news, and personal information.

> "Even the most aggressive antitrust actions that target alleged abuses of platform market dominance are unlikely to squarely address the political threats that concern us."

Perhaps for these reasons, some have suggested that the antitrust laws might force divestitures of certain assets of the platforms, perhaps even breaking them up into smaller constituent parts along their separate lines of business. But it isn't clear that even significant divestitures of the platforms would mitigate their political power, so long as they retain the central internet platforms and ability to control what users see. Although separating the platforms from ancillary revenue streams would reduce their financial resources and make them dominant in fewer markets, the source of their political power would largely remain intact. Moreover, because of network externalities and related features of digital platforms discussed in Section II of this report, the platforms will maintain their dominance against rivals so long as market forces advantage platforms with greater scale. Even if the platforms themselves were broken into multiple smaller platforms, network effects and scale economies might result in the markets tipping back to a single dominant platform and thus

[††] Amazon rolled back this price parity policy in the EU after antitrust scrutiny in 2013 and completely eliminated it from its contracts with third-party sellers in 2017. However, Amazon's Fair Pricing Policy allows the company to retaliate. See Guadalupe Gonzalez, "You're No Longer Required to Sell Products for Less on Amazon. The Problem? If You Don't, You've Got Another Penalty Coming," *Inc.*, March 13, 2019, https://www.inc.com/guadalupe-gonzalez/amazon-removes-price-parity-not-fair-price-rule-third-party-sellers-antitrust-violations.html.

the same political problems as those faced today. Thus, even the most aggressive antitrust actions that target alleged abuses of platform market dominance are unlikely to squarely address the political threats that concern us.

Enhanced merger review

Merger review has been perhaps the chief target of those who criticize the inadequacy of antitrust enforcement against the dominant platforms. Many attribute Facebook's continued dominance to its acquisitions of WhatsApp and Instagram and Google's monopolistic control of digital advertising to the company's purchases of DoubleClick and YouTube.[22] Critics of those acquisitions argue that they involved a dominant platform's purchase of a would-be rival and thereby sustained or enhanced monopolistic control of potentially competitive markets. These remarks echo general calls for increasing scrutiny of mergers in innovation-sensitive markets, especially when the acquiring party controls a digital platform. Some commentators have advocated for shifting the burden of proof to require the acquiring party to convince decision-makers that an acquisition would not cause harm to competition, rather than requiring enforcers to prove that it would.[23] Some have asked for aggressive retrospective reviews of acquisitions that appear problematic and for corresponding divestitures.[24] Others have asked for a blanket prohibition of all acquisitions by dominant platforms.[25]

To the degree that heightened scrutiny of mergers might increase the likelihood that a targeted firm would, instead of being acquired, remain independent and pose a genuine competitive threat to a dominant incumbent, more aggressive merger policy might prevent platforms from amassing and entrenching dangerous political power. But improving merger policy per se would do little to mitigate the political harms that current platforms pose. If Facebook's acquisitions of Instagram and WhatsApp are retrospectively found to be illegal, and a divestiture is deemed to be an appropriate remedy, then Facebook's control over information exchange in social media markets might be mitigated, but the company would still enjoy control over vast information networks. The threat of political harms might be lessened, but probably not eliminated.

In sum, improving merger review in acquisitions involving digital platforms might provide economic benefits in certain markets, but it is not likely to get at the core challenge of mitigating the political harms that today's dominant platforms pose.

Targeting anticompetitive information acquisition

Because the source of power for the digital platforms lies primarily in their acquisition and utilization of data, perhaps antitrust actions that target the anticompetitive acquisition and control of personal information, or other anticompetitive conduct that increases the platforms' access to data, could offer protections against some of the political dangers of platform dominance.

One such action might target Google's acquisition and monetization of personal information. Critics have argued that Google employed exclusive contracts and other exclusionary conduct to expand and secure the dominance of its search engine on browsers, smartphones, and websites.[26] The company uses its search engine, along with its other offerings (e.g., Google Maps, Gmail, and other customer-facing properties) to acquire vast amounts of personal data about its users, which it then uses to sell targeted advertising services. If Google is found to have unlawfully enlarged or maintained a monopoly in search, the remedy might restrict the company's ability to use that data to advance its other businesses. Perhaps Google might also be prohibited from similarly collecting intrusive personal data in the future. Either remedy would loosen Google's control over users' personal information.

Facebook's business model also gathers and monetizes personal information. Although the company gathers user data from its Instagram, WhatsApp, and other products, Facebook's primary information source is built atop its dominant social network. Some have suggested that the company obtained its dominant status by engaging in a number of deceptive practices. In an influential article, Dina Srinivasan reports that Facebook misled both Facebook users and Facebook competitors at a time when alternative social network platforms were available.[27] First, Facebook allegedly misled its users when it promoted itself as a platform committed to protecting user privacy.[‡‡] In part on the basis of these assurances, Facebook emerged as the platform preferred by users and—reflected in the winner-takes-all nature of digital competition—came to dominate the market. And after Facebook became the dominant social network site, according to Srinivasan, it diluted its privacy protections and sold user data, contrary to its prior assurances. In what amounted to a reneging of prior pledges to consumers, Facebook could offer its user data—data that no other social network possessed—to advertisers and profit heavily. In short, once users were locked into their Facebook profile, the platform enjoyed a durable monopoly that allowed the company to use personal data in ways contrary to its promises and charge higher prices to advertisers.

Although merely breaching a promise that was not fraudulent when made probably does not violate the antitrust laws, there might be an antitrust claim if Facebook engaged in fraudulent conduct that was designed to capture monopoly power and foreclose the market to more efficient rivals. If such a claim were not barred by the statute of limitations and were substantiated at trial, it could be very significant: unlike the other potential antitrust actions discussed herein, this claim targets conduct that led to Facebook's original dominance. An appropriate remedy might be to unwind the gains in market share that Facebook now enjoys

[‡‡] For example, Facebook made repeated assurances that it would not use plug-ins to track users or collect their data. These assurances turned out to be false, but the false assurances allowed Facebook to grow market share at a time when there was still substantial competition between alternative social networking sites. Additional evidence suggests that Facebook was privately using data to target ads at the same time it was denying it publicly.
In addition, a 2010 report revealed that every time a Facebook user visited a page with a "like" button, Facebook retrieved the user's Facebook login cookies, contrary to user assurances. This additional user data may have aided Facebook in selling higher-priced ads.

because of its deceptive practices. Although it is hard to foresee how such an unwinding would take place—which platforms would emerge in Facebook's stead, and what would happen to all of Facebook's acquired data—an antitrust remedy based on such an action could in principle reduce the political dangers Facebook poses.

"We do not intend to denigrate the importance of sound, aggressive antitrust enforcement, but we question the extent to which it can meaningfully correct the political and social problems that are also of primary concern."

Antitrust actions that, if successful, curtail the dominant platforms' ability to acquire and utilize personal information from users might address concerns over the political dangers they currently present. However, any success along these lines remains deeply uncertain, and a more likely outcome would be similar to other antitrust actions, which might limit the companies' future anticompetitive conduct and influence on ancillary markets but would not substantially weaken the core business models or market positions. We do not intend to denigrate the importance of sound, aggressive antitrust enforcement, but we question the extent to which it can meaningfully correct the political and social problems that are also of primary concern.

B. Reforming Antitrust's Consumer Welfare Standard

Since the rise of the Chicago school in the 1970s, antitrust law has increasingly been honed to pursue economic objectives: to redress anticompetitive conduct and to advance economic welfare. Although the so-called consumer welfare standard has come under frequent attack,[28] it has prevailed both in courts of law[29] and among most antitrust scholars.[30]

The rise of dominant internet platforms has renewed criticism of the consumer welfare standard. Because the dominant platforms pose both economic and non-economic threats to American consumers, some have argued that antitrust law must be retooled to confront a wider set of policy challenges in the platform age. This would require expanding antitrust's domain beyond economic concerns to include a variety of political values.

To be sure, antitrust law has always been built atop a foundation of democratic political values. Competitive markets disperse economic power, thereby limiting the ability of private firms to use economic power for political favors.[31] Conversely, entrenched monopolies are known to fester within our political economy, corroding the operation of both markets and politics. If antitrust enforcement can keep markets competitive, the theory goes, it will help keep democracy vibrant. Luigi Zingales has warned that the past decades' growth of

economic concentration and corporate influence, in part due to inadequate antitrust enforcement, has created a "Medici vicious circle" in which economic and political power reinforce each other.[32]

Recent enthusiasts of expanded antitrust enforcement, however, want antitrust policy to act on political and social values more directly. Some have argued that the antitrust laws should police—and ultimately break up—the nation's largest companies measured by financial assets, regardless of whether they have monopolized markets or engaged in anticompetitive conduct.[33] Others have suggested that antitrust law should protect small producers against the success of their large competitors, even if the economic woes of the smaller companies are due to their inefficiencies. And some have said that antitrust law should protect non-economic values, such as privacy or free expression, and thus should require large companies to provide services and protections that the marketplace does not seem to demand.[34] These proposals to use antitrust law to rectify income inequality or curtail corporate power are part of what has been called a "neo-Brandeisian" antitrust movement.

Though we sympathize with many of the motivations that underlie these proposed changes to antitrust law, we are concerned that expanding antitrust law beyond its economic focus would invite damaging policy incoherence. In the first place, expanding the objectives of antitrust law would matter only when doing so would lead to different enforcement decisions and thus result in outcomes that reduce economic welfare. Courts would be forced to awkwardly balance incommensurate values. Similarly, revising antitrust laws to protect small or less wealthy producers would put the government in the position of allocating surpluses to producers or consumers in a zero-sum (or negative-sum, to the extent the redistribution imposes costs or reduces incentives for welfare-enhancing conduct) relationship. There is no algorithm for reconciling the competing objectives. As a result, antitrust decisions would be seen as arbitrary, undisciplined, and incoherent, and their legitimacy would be questioned. Moreover, a less coherent, less principled body of antitrust law would be less effective in restraining the discretion of courts and enforcement agencies. Antitrust law would thus be subject to greater risk of regulatory capture, which is likely to benefit the wealthy and powerful.

Recent events suggest some of the dangers that might arise. President Trump's campaign against CNN as a purveyor of "fake news" was alleged by some to have influenced the Department of Justice's attempt to block AT&T's acquisition of Time Warner.[35] A policy to alleviate regulatory burdens on automobile manufacturers caused the Trump Administration to curtail California's environmental regulations, and when it later investigated possible antitrust violations by automakers that sought to comply with California's higher standards, it was accused of using antitrust law to further its environmental policies.[36] The Justice Department invoked national security when it intervened on behalf of Qualcomm, and in opposition to the Federal Trade Commission, to argue that imposing antitrust remedies on Qualcomm for anticompetitive monopolistic conduct would jeopardize the United States'

leadership in 5G technology.[37] And it has been alleged that concern about drug use motivated the Justice Department to challenge proposed mergers of marijuana manufacturers that did not raise legitimate antitrust concerns.[38] In all of these instances, critics questioned whether the Justice Department was motivated, not by antitrust law and policy, but by other, unstated objectives.

We do not know whether these criticisms are well founded, but we do know that law enforcement and political institutions in general are undermined when the motives and legitimacy of law enforcement actions are questioned. Laws with competing objectives but lacking clear guidelines for reconciling those objectives are likely to give rise both to such questions and to the kinds of abuses that provoke them.

Although we believe that dominant internet platforms pose threats to American society and democracy that are beyond the reach of the nation's antitrust laws, we do not recommend changing antitrust law to address those threats explicitly. Instead, we propose developing additional regulatory tools and preserving the focus of antitrust law on economic welfare.

C. Requiring Data Portability and Interoperability

A number of groups investigating platform dominance, including the European Commission and the authors of the Competition Law 4.0 report, have suggested that data portability might be a way to increase competition among internet platforms. As an example of an American portability policy, mobile phone providers were required to allow consumers to keep their numbers when switching from one carrier to another. The policy prevented locking in customers and encouraged competition among carriers. A data portability requirement has been built into the EU's GDPR, which mandates that there be a standardized, machine-readable format for the transfer of personal data.[39]

Requiring data portability can be an important policy response to address a number of social harms. It can give individuals greater agency by providing the ability to remove themselves from platforms and engage only in voluntary relationships vis-à-vis their data. Portability might also prevent platforms from locking users into their platform and coercing use of additional services.

As a strategy to enhance competition, however, the effectiveness of data portability may be more constrained, in part because of the limited character of the data that can plausibly be moved. The GDPR's Article 20, for example, applies only to data given to the platform by the user, which includes information such as name, address, credit card information, email address, and the like, but would not necessarily include all of the metadata generated by the user's interaction with the platform. This metadata includes likes, clicks, browsing history on the platform website, order history, searches, records of returns, or consumer complaints. In the case of a Facebook user, it would include the user's friends.

Metadata is particularly valuable for targeted advertising, making it particularly meaningful in terms of economic power and competition. The types of metadata generated by a user are very platform specific and therefore heterogeneous: on Facebook it is your circle of friends; on eBay it is your positive feedback score; on TikTok it is your posts, which in most cases is a music video; on Twitter it is your tweets, likes, and retweets. Unlike simple user data such as names, email addresses, or mobile phone numbers, it is not clear how metadata from one platform could be converted into a form that would be useful on another. Much of the content of the metadata you generate, like the emails you write or searches you undertake, would be unusable without considerable further processing. The GDPR requires the "processor" (i.e., platform) to write a specialized import-export module (EIM) to translate data into other formats; this would either substantially raise the compliance costs to a small competitor, or exclude the data from transfer altogether since the GDPR exempts from its portability rules data that is not technically feasible to transmit (without defining what feasibility means).

It may be possible to specify data formats for specific sectors. For example, much work has already been done to develop standardized data records that would allow users to switch banks or health care providers. But the big social media platforms present a different challenge since the data templates for Twitter, Facebook, and search engines differ significantly, and future digital offerings are likely to introduce new templates. Seeking standards to facilitate data sharing is unlikely to tap into the data resources that underlie the platforms' source of market power.

"Policy measures seeking to protect consumers from internet platforms will need to take into account the interplay between advancing competition and protecting personal privacy."

In addition, as we noted previously, requiring data sharing in order to stimulate platform competition can also be in tension with other social objectives, such as user privacy. Users could transfer their own data to various smaller social networks (so-called "multihoming"), but they would not be able to also transfer their friends' data without the friends' explicit consent. While these niche networks might flourish alongside Facebook, for example, it seems likely that many consumers will prefer to remain on a large platform with a diverse set of present and past acquaintances—thereby allowing the largest platforms to maintain their dominance. As a general matter, threats to privacy will increase the more private data is shared across entities. Policy measures seeking to protect consumers from internet platforms will need to take into account the interplay between advancing competition and protecting personal privacy.

An alternative to requiring data portability is requiring interoperability. Under this approach, data would stay with the platform that collected them, but competitors would be allowed to have real-time access to both the data and the metadata generated by the platform. Such access might allow rivals to tap into the dominant platform's network effects, benefit from its scale economies, and pose genuine competitive challenges. This is what Zynga once did with its game FarmVille, an app that rode on top of the Facebook platform. The game could be played only within Facebook, which provided users with access to Facebook's data, including their friends. Facebook, however, was very careful to limit FarmVille's functions to those it thought would generate complementary services and forbade FarmVille from competing with core Facebook functions such as messaging. Facebook and other platforms would have to be compelled to share its application programming interfaces (APIs) more broadly for real-time access to data and metadata. And, to be effective, the remedy would have to require maintaining open APIs that outsiders could utilize; that requirement might retard, or at least increase the cost of, platform innovation and product improvements.

As we explain below, the proposed middleware remedy builds on a version of this approach. The remedy might come in two forms: a voluntary one in which the platforms permit third parties to provide filters to the information the platforms generate, subject to limitations they place on the kinds of data that can be shared; and a more coercive one in which the platforms are required by statute to provide more complete access to their APIs.

D. Enhancing Privacy Protections

We have pointed out the harm that internet platforms cause consumers by violations of their privacy. Indeed, the platforms' business models revolve around using consumers' personal data to sell advertising: the more data they have, the more widely and accurately they can target ads, and their possession of huge troves of personal data gives them overwhelming advantages against competitors in the marketplace.

"Privacy law can limit the degree to which a platform can use consumer data generated in one sector to improve its position in another, thereby both limiting the use of consumer data and restraining a source of competitive advantage."

Expanding consumer privacy protections might deter some platform abuses. Privacy law can limit the degree to which a platform can use consumer data generated in one sector to

improve its position in another, thereby both limiting the use of consumer data and restraining a source of competitive advantage. As noted earlier in this report, digital markets are different from previous product markets precisely in this sense: there are strong returns to scale and scope in the possession of consumer data; the more data a platform has, the easier it is to generate higher revenues and more data.[§§] Possession of this mass of data helps the platforms move into not just adjacent markets but also completely different ones where they have no experience.

Amazon, for example, was able to move from marketing books to marketing baby diapers and groceries because it already possessed enormous data about its customers. Google reportedly has amassed a huge database in which it has combined information from its different products—Chrome, Gmail, Google Maps, and its search engine—into a single master record of each individual who has used its services.[***] The company can combine shopping preferences with political views, physical location, and movement to track individuals. The uses of aggregated data can enable product improvements and other benefits. But they also risk privacy harms because, though the data is supposedly anonymized, it would be easy to correlate it with specific individuals, particularly if it includes location data.

There are existing limitations on the ways a platform can use personal data to move into a different market. The GDPR places restrictions on the collection, processing, and use of data and states that consumer data can be used only for the purpose for which they are originally collected, unless the consumer provides explicit permission to the platform.[40] This would, in theory, prohibit the large platforms from moving into new markets using their data advantage, or at least slow them down considerably as they sought to get permission from existing consumers. Privacy law applied in this fashion can restrain the dominance of the largest platforms. In 2019, the German Bundeskartellamt ruled that Facebook violated both German competition law and the GDPR when it combined user data from its social network, other Facebook services, and third-party websites.[41] The German Federal Court of Justice affirmed the decision in 2020 but focused on the competition law violation, ruling that aggressive data collection efforts amounted to an abuse of monopoly power because they were contrary to consumer preferences. While European regulators are likely to continue exploring how combinations of privacy and competition law might limit how internet platforms gather data in an effort to restrain their economic might, the kind of legal theory on which the German court relied has no real counterpart in US law.

Relying on privacy laws like the GDPR to constrain these commercial strategies can, however, present some issues. It is not clear whether the GDPR applies only to data that the consumer

[§§] For a contrary view, see Marco Guerzoni and Massimiliano Nuccio, "Big data: Hell or heaven? Digital platforms and market power in the data-driven economy," *Competition and Change* 23, no. 3 (2019): 312-328.

[***] This practice has been challenged in Europe. See Kimberly A. Houser and W. Gregory Voss, "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?" *Richmond Journal of Law and Technology* 25, no. 1 (2018): 5-109.

voluntarily gave to the platform (e.g., email address, name, mailing address, and credit card information), or also to metadata about the consumer's interactions with the platform (clicks, likes, links followed, etc.). Was this data voluntarily surrendered by users and therefore their property, in effect, or does it belong to the platforms since they played a role in generating it? Any law that limits data use will need to address these kinds of difficult questions about the specific data categories to which it applies and about what constitutes improper use.[42]

Another issue is that, as some have put it, the cat is to some extent already out of the bag. Google and Facebook have already amassed huge quantities of customer data.[43] Some of that data was allegedly acquired illegally; Facebook, for example, collected browsing data from its users when they were outside of Facebook. It signed a consent decree with the FTC to stop but continued to collect this data in violation of the agreement. Perhaps the FTC could require the company to erase this data, but enforcing compliance to such an order would be difficult, and in any event, regulators do not know how much data these large platforms have.

"Just as we do not want measures such as requiring data sharing that promote competition but harm privacy interests, we do not want privacy laws to harm competition."

Policymakers must also be alert to the concern that an expansion of privacy law could simultaneously have the effect of strengthening the market dominance of today's internet platforms. A privacy law that prevented internet companies from using consumer data to move into new markets could have the greatest effect on smaller platforms that need to amass data to properly compete with Google and Facebook. Although there remains a question about the continuing value of "old" data,[44] adding muscle to privacy law after the large internet companies have already gathered consumer data could have the effect of enshrining their market leadership and thereby hurting would-be competitors.

Finally, the GDPR is a hugely complicated law, compliance with which has employed a legion of lawyers in multiple jurisdictions to help platforms protect themselves. This too can reward large incumbents and penalize smaller would-be competitors. Just as we do not want measures (such as requiring data sharing) that promote competition but harm privacy interests, we do not want privacy laws to harm competition.[45]

In sum, without denigrating the significance of privacy laws to protect consumers and society, we believe for the reasons outlined above that privacy laws are limited in their ability to curtail the market power, and thereby the political power, of the dominant platforms. While it may be possible to restrict the use of new consumer data by platforms, the large

existing platforms already possess huge amounts of such data, and restriction on acquisition or use of data may harm their competitors more than the established giants.

E. "Middleware" as a Structural Solution

> *We need to open up and be transparent around how our algorithms work and how they're used, and maybe even enable people to choose their own algorithms to rank the content or to create their own algorithms, to rank it. To be that open, I think, would be pretty incredible. So that we can all come to better solutions, because it affects society in such large ways.* — Jack Dorsey, Twitter CEO, August 8, 2020 [46]

Very few policymakers have considered pursuing structural interventions to stem platform dominance, but we think technological interventions might offer the most promising remedies. Specifically, we propose stimulating the creation of a competitive layer of companies offering middleware products. Although middleware is traditionally defined as computer software that provides services beyond those available from an operating system, including the software that connects operating systems with applications, we use the term to include software and services that would add an editorial layer between the dominant internet platforms and consumers.

"We view middleware as an opportunity to introduce competition and innovation into markets currently dominated by the principal internet platforms."

In antitrust circles, the concept of middleware was popularized in *United States v. Microsoft* (2001),[47] which referred to software products that interconnected with Microsoft's Windows operating system through APIs. Middleware products written for Windows had the capacity to supersede some or all of Windows' platform functions; other software could then be written directly for the middleware, rather than for Windows. The middleware thus served as, or provided input to, an alternative platform for other software, thereby undermining Microsoft's monopoly on the operating systems market. The core of Microsoft's antitrust violation was its restrictive conduct that limited the growth of middleware, including Java and Netscape Navigator.

We view middleware as an opportunity to introduce competition and innovation into markets currently dominated by the principal internet platforms. There is enormous pressure on the platforms to filter from their domains not just illegal content, but also material that is deemed politically harmful, such as conspiracy theories, fake news, and abusive content. As noted in the Introduction of this report, this kind of political content curation is done

routinely by traditional media companies, but it is altogether different to give these duties to dominant internet platforms—private companies that unilaterally control vast swaths of communication through highly non-transparent means. Indeed, those platforms have often been reluctant to play this role. A competitive middleware sector would help solve this problem by outsourcing content curation to other organizations that enable consumers to tailor their feeds to their own explicit preferences. At the same time, middleware, in our view, could be a superior alternative to structural remedies imposed by either courts or regulators, in that it would directly respond to consumer preferences and market actors.

The nature and function of middleware

By "middleware," we refer to software products that can be appended to the major internet platforms. These products would interconnect with Facebook, Amazon, Apple, Twitter, and

"Middleware, in our view, could be a superior alternative to structural remedies imposed by either courts or regulators, in that it would directly respond to consumer preferences and market actors."

Google APIs and allow consumers to shape their feeds and influence the algorithms that those dominant platforms currently employ. Middleware would not necessarily disintermediate services between the consumer and the internet platform; rather, as a third-party service chosen by the consumer, it would make editorial judgments that are currently provided (usually without transparency) by the platform. This relationship between middleware and a platform is illustrated in Figure 4. Alternatively, middleware could offer an independent entry point into the platform (though the platforms would likely oppose losing the point of service to the customer). In short, users could utilize middleware via a platform or access a platform via middleware. In either case, middleware can tailor the functionality of those websites to the preferences of their users.

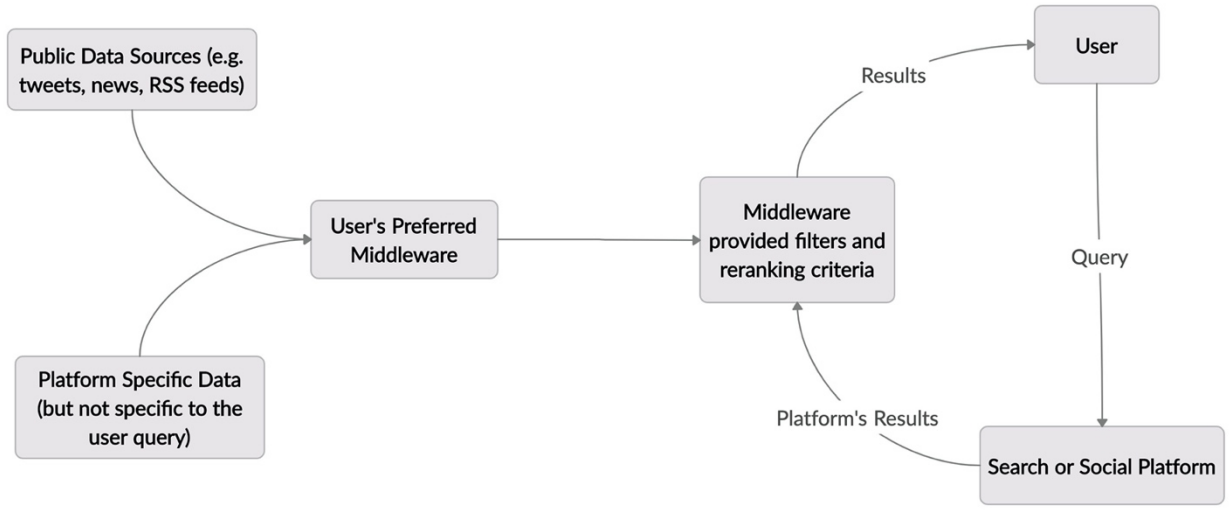


Figure 4: *How middleware will interact with a platform's functions. Note that no user data flows to the middleware provider.*

"By mediating the relationship between users and the platforms, middleware can cater to the preferences of individual consumers while providing significant resistance to unilateral actions by the dominant players."

We imagine a diversity of middleware products, designed to accommodate the individual platforms and meet specific demands of interested consumers, with transparent offerings and technical features so that users can make informed choices. Middleware can offer fact-checking services, news rankings, relevance priorities, information filters, or other services that supplement those currently supplied by the major platforms. Similarly, middleware could adjust news results from Google searches and Facebook pages. While our focus here is on politically related content, middleware can also give users more control over commercial content and privacy settings. For example, consumers could select middleware providers that adjust their Amazon search results to favor domestic production and eco-friendly products, or that make fine-grained choices on Facebook's privacy settings dashboard. Trusted community organizations or preferred media organizations could offer, sponsor, or endorse middleware providers. Platforms could also offer their own middleware, on the condition that they do not favor their own product over those provided by third parties or make their own middleware a default choice. By mediating the relationship between users and the platforms, middleware can cater to the preferences of individual consumers while providing significant resistance to unilateral actions by the dominant players. To the extent that the middleware

increases the value of the platform to consumers, it should generate economic rewards for the platform as well as the middleware provider and the consumer.

Figure 5 illustrates a type of middleware we envision. Google searches often offer highlighted news stories related to the search subject, but the algorithms that generate recommended stories are opaque. Consider three Google searches for “Amy Coney Barrett,” each one producing a different list of recommended news stories:

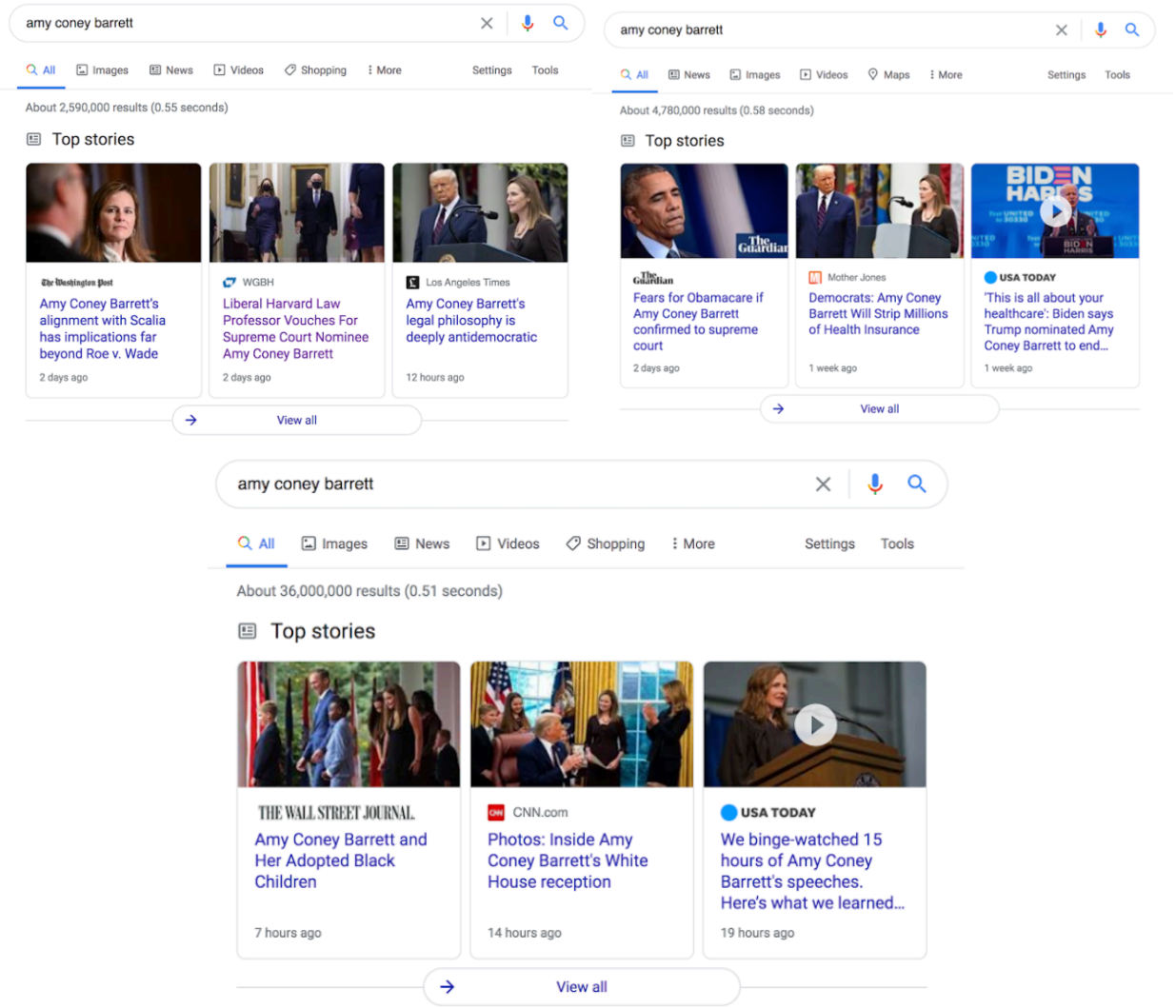


Figure 5: *Screenshots of three different results of a Google search for “Amy Coney Barrett” with different recommended news stories.*

Our envisioned middleware add-on to Google would give the user greater control over the news recommendations that Google searches generate for that particular user. The middleware service would provide labels (such as “misleading,” “hate speech,” or “lacks context and should be read in conjunction with__”). Middleware could also offer relevance

scores when users conduct a Google search, ranking news stories seen by the user and affixing labels to each news story. Hence, by selecting a preferred middleware provider, the user could prompt a Google search to recommend stories that pertain to their particular interests, meet certain journalistic standards, or fit dimensions of timeliness or age appropriateness. If the user does not like the recommendations generated by a particular middleware filter, they can select an alternative. The middleware remedy allows users to shape the hidden algorithmic processes and assert greater control over what they see.

Middleware can also offer a variety of interventions, ranging from nominal to more significant. A minimal role for middleware could simply be to add labels to platform outputs without removing content, such as labeling certain Twitter posts as "hate speech," certain Facebook news feeds as "unverified," or certain Amazon products as "produced in the USA." A more interventionist middleware might influence the rankings for certain feeds, such as Google searches, Facebook advertisements or news stories, Amazon product lists, or YouTube video recommendations. An even more assertive middleware could hide certain content, or block specific information sources or manufacturers altogether. Users could both select the producer of the middleware and adjust the form of middleware intervention. In order to ensure that middleware does not facilitate repression, perhaps by autocratic regimes, such services should be opt-in only and designed to prevent censorship.

"Middleware's primary benefit is that it dilutes the enormous control that dominant platforms have in organizing the news and opinion that consumers see."

Advantages of employing middleware

Middleware's primary benefit is that it dilutes the enormous control that dominant platforms have in organizing the news and opinion that consumers see. Decisions over whether to institute fact-checking, remove hate speech, filter misinformation, and monitor political interference will not be made by a single CEO but will instead be controlled by a variety of informed and diverse intermediaries. For this reason, technology companies—who have expressed an eagerness to outsource some of these decisions—may be willing to embrace controlled offerings of middleware, since it will afford them the space to focus on their core mission, rather than having to determine (and defend) decisions that so significantly affect the information that millions of users consume.

Additionally, middleware facilitates competition. It offers a new and distinct layer of potential competition for consumer loyalties and opens a pathway for innovations in managing information, including commercial information that might benefit firms otherwise disadvantaged by the platforms' business models. It could also open lucrative markets both

for technology companies that can improve platform functionality and for civic organizations that want to participate in political and social discourse.

Finally, a middleware system could offer services that many in our society deem to be urgently needed, such as a robust system of fact-checking and hate-speech moderation. Current platforms hesitate to provide these services because they know their decisions are so consequential and that various people do not trust the motives of the fact-checker. When these services are instead offered by a diversity of providers, no one player exercises outsized power in making fine-grained decisions over content, and users can select providers they trust. Allowing users to choose from multiple middleware providers offers a blueprint for bringing transparency and flexibility to privacy settings, terms of service, and other services that users care about.

Although many platforms already tailor algorithms and customize feeds to meet users' interests and past practices, our middleware proposal is far more substantive than these current practices. Middleware completely removes the platforms' currently enormous editorial control over organizing political content and labeling or censoring speech, and it enables new providers to offer and innovate in services that are currently dominated by the platforms.

There is a standard objection to any effort that would fragment the internet and allow groups to reinforce filter bubbles around themselves. While universities might require their students to use middleware products that direct them to credible information sources, conspiracy-minded groups might do the opposite. Empowering each individual to tailor their algorithms might encourage a further splitting of the American polity, allowing groups to more easily find voices that echo their own views, sources that confirm their factual beliefs, and political leaders that amplify their own fears.

These concerns are serious, but in our view, they can be mitigated by robust regulation, as we discuss below, and are outweighed by the dangers of concentrated platform power. It must first be acknowledged that it is technologically impossible to prevent such splintering. Many conspiracy theorists like QAnon followers, for example, abandoned the big platforms and migrated to the 4chan message board to seek common voices, and when 4chan moderation teams started tempering incendiary comments, the conspiracy theorists moved to a new platform, 8chan (and later, after 8chan was deplatformed, to 8kun).[48] They could continue to communicate with one another on encrypted channels like WhatsApp, Telegram, or Signal, or indeed through ordinary email. Moreover, however problematic these gatherings are, they tend to involve individuals who voluntarily subject themselves to the views expressed, and their right to do so is in fact protected by the First Amendment. The only restrictions to this right come into play when they encourage violence or criminal activity, which would of course apply to any middleware product.

Perhaps most important, extremist groups become dangerous to democracy primarily when they leave the periphery of the internet and enter into the mainstream, either by being picked up by the mainstream media, or—what we are primarily concerned with—having their voices dramatically amplified by a platform's ability to propagate viral messages. A dominant platform, unlike 8chan, has the ability to influence what informs a broad swath of the population, against their will and without their knowledge. Many people dream about an internet in which the large platforms moderate content according to *their* political preferences, returning us to an age in which Walter Cronkite determined what facts and opinions Americans heard. But while platform power could be used for what we today might regard as good purposes, it could also be used for bad ones down the road. The long-term problem for our democracy is the existence of such concentrated power in the first place, not the way it is used in the short run. For this reason, the greater danger, we believe, is in the unaccountable power that dominant platforms possess, rather than from any splintering that would occur from competition among many platforms.

Questions to be answered and the role of regulation

Although we are enthusiastic about middleware solutions, we recognize that implementing this structural adjustment to internet platforms will first require answering important questions. We explicitly acknowledge that we offer here only a conceptual outline of a middleware approach and that much thinking remains to be done. To start, we highlight three aspects of a new middleware architecture that will require careful elaboration.

First, the role and function of middleware must be determined. We emphasize that, whether by statutory authority or by consequence of a consent decree, we consider it necessary to mandate that dominant search engines and social media companies allow users to choose among third-party filters. Moreover, the platforms might be compelled to alert users to the option of installing middleware and to require users to explicitly opt out of middleware use. Middleware can serve its intended purpose only if it is used widely, and a default option that allows users to never consider installing middleware would severely limit its uptake.

Even under these mandatory rules to encourage middleware adoption, the division of responsibility between the dominant platforms and the middleware filters could vary. At one extreme, the middleware performs all of the essential functions—such as procuring content, sequencing results, and distributing feeds—and the underlying platform serves as little more than a neutral pipe. At the other extreme, the platform continues to curate and rank the content with its standard algorithms, and the middleware merely serves as a supplemental filter to the platform's output, such as by tagging specific pieces of content with labels or warnings. It is unlikely that either of these extreme arrangements would be satisfactory; the former would likely prompt aggressive resistance from the current platforms because it would undermine their business and revenue models (and perhaps future innovation), while the latter would likely be inadequate to curb the dominant platforms' power in curating and disseminating content. An intermediate role would probably be preferable.

One intermediate role might be that middleware both provides filters for specific news stories and develops ranking and labeling algorithms, which are then integrated into the main platform. Developing this intermediate role would require further reflection, both from a regulatory point of view and in terms of technical architecture. Congress would likely have to pass a law requiring platforms to use open and uniform APIs—the software interconnects that would allow middleware companies to receive content seamlessly from a multitude of tech platforms and provide labels and recommendations back to these platforms without requiring duplication of effort. Middleware should additionally be subject to some minimal standards, so as to preclude criminal or other nefarious conduct and to ensure that middleware providers follow a consistent and transparent approach. These standards could adhere to guidelines outlined by a regulator or to rules set up by the platforms themselves. Though allowing the platforms to set the standards for middleware could undermine their value, it might also advance robust parameters that assure consumers and provide guardrails to minimize the negative effects of filter bubbles.

Second, a business model for middleware providers must be sufficiently attractive to induce an adequate supply. The most logical approach would be to establish revenue sharing arrangements between the dominant platforms and the third-party providers of middleware. If a middleware product enhances the value of the platforms to users, the platforms might be able to generate increased advertising (or maybe, in the future, user fee) revenues that could be shared with the middleware provider. Alternatively, the middleware provider might be able to charge user fees or sell advertising directly.

“A technical framework must be developed that would invite a diversity of middleware products.”

If a middleware product reduces the value of the platform, by, for example, making it harder for the platform to optimize the targeted advertising or by losing advertising revenues to middleware providers, the platforms will predictably resist a middleware requirement. Middleware might have to be offered as an alternative to more onerous regulatory requirements or legal risk related to their role as providers of political or otherwise offensive information. And if middleware providers are not able to obtain revenues directly or by sharing platform revenues, the terms of such revenue sharing might have to be established by regulators. The negotiated fee sharing must navigate a balance between encouraging the development of a robust supply of trustworthy middleware while also inducing the cooperation of (or avoiding hostile refusals from) dominant platforms and preserving their rewards for investment in and innovation on the platforms.

Third, a technical framework must be developed that would invite a diversity of middleware products. The technological requirements for a vibrant middleware market might be

demanding. Middleware developers must be able to easily deploy their products to work with the various dominant platforms, each of which exhibits different architectures, as well as with other closely related platforms. At the same time, the specifications for middleware should be sufficiently simple that a diversity of technologists and nonprofits can sponsor offerings. Moreover, middleware must be prepared to assess at least three different kinds of content: widely accessible public content, including news stories with RSS feeds and tweets from public officials, that already has an identification system for searches and aggregators; public content generated by users of social media networks and search engines that is curated on those platforms, which the platforms must make available and cognizable to third-party providers; and content that is not public but nonetheless might attract the attention of either middleware or platform monitors, such as WhatsApp messages that promote hate speech or individual Facebook posts that encourage violence. Third-party providers will have to identify these different kinds of content and then offer their assessments of, for example, veracity, relevance, or centrality to whatever metric the middleware provider is applying. Because the middleware provider will not have access to private content, middleware services may have to provide labeling algorithms on top of features provided by the platform. Navigating these categories of content and providing consistent services will pose a challenge to third-party providers.

It is critical to get these technical elements right. The middleware intervention would be appropriately questioned if it generated an inadequate supply and diversity of third-party providers, became another tool to capture control over public discourse, or introduced more technological bottlenecks. We believe that a middleware solution has the potential to reduce informational and economic concentration, as long as the technical solutions offer an intuitive and open architecture that fosters a diversity of middleware suppliers and products.

"American regulators need to accumulate the requisite expertise and develop the appropriate policies that meet the demands of the digital economy."

F. A Specialized Agency

Several commentators, in observing that the dominant platforms pose daunting policy challenges that require a high degree of technical expertise, have proposed that the United States create a specialized agency dedicated to regulating the giants of the digital economy. The Stigler Center report, observing that competition in internet markets presented economic dynamics and technical difficulties that are distinctive from the rest of the economy, recommended considering the creation of a "Digital Authority" that would acquire sector-specific expertise and issue sector-specific rules.[49] An expert report co-authored by

Jason Furman and submitted to the United Kingdom's Competition and Markets Authority (CMA) recommended constructing a "digital markets unit," either as a stand-alone entity or a specialized body within the CMA, to establish industry codes of conduct that sustain innovation while guarding against anticompetitive and other forms of harmful conduct.[50] A whitepaper from the Shorenstein Center at Harvard's Kennedy School recommended establishing a "Digital Platform Agency" to meet what it describes as new digital realities.[51] For essentially the same reasons, we agree with these calls for developing a specialized agency to address the challenges posed by the dominant platforms. American regulators need to accumulate the requisite expertise and develop the appropriate policies that meet the demands of the digital economy.

Our middleware proposal, if adopted, heightens the need for additional agency expertise. Prior calls for a specialized agency identified the need for greater regulatory proficiency in understanding the economics of digital markets, appreciating the many uses of personal data and associated threats to privacy intrusions, anticipating the pace and direction of technological change, and recognizing the industry- and economy-wide benefits of establishing common technological and consumer protection standards. In addition to these needs, our middleware proposal would also demand of regulators the capacity to ensure, or if necessary mandate, the availability of platform APIs to middleware providers, platform compliance with other conditions necessary to allow middleware providers to offer their products, and fair revenue sharing and adherence to rules that allow middleware business models to thrive. Even more challenging, administrators of our middleware proposal will need to work with industry leaders to chart out the assorted responsibilities and prerogatives for both middleware providers and the platforms and to design the technical framework that will allow middleware offerings to thrive.

It is unlikely that a consent decree, court-ordered remedy, or existing statute provides the authority to establish the kind of agency we envision, even if such an agency were housed in an existing administrative body like the FTC or FCC. We expect that Congress would have to pass a statute that establishes a new specialized agency with the expertise and resources described herein and charges that agency with many of the policymaking powers required to foster a middleware market. However, any new statutory authority does not need to be expansive, nor would it be necessary to disrupt or reorganize the operations of other parts of government. An advantage to the middleware proposal is that it leaves most other policy instruments unchanged. Therefore, implementing our middleware proposal and building the administrative capacity needed to administer it would require a statute that describes the purpose and objectives behind instituting middleware, issues the required mandates to dominant platforms, and invests in an agency with the technical expertise to research policy solutions and the rulemaking authority to achieve Congress' goals.

V. Conclusion

The public should be alarmed by the growth and power of dominant internet platforms, and particularly by their control over political speech. 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 take editorial power away from a small number of technology platforms and hand it not to a single government regulator, but to a diverse group of competitive firms that would allow users to tailor their online experiences."

Today, 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 while antitrust law may be effective in mitigating certain economic abuses, it is not necessarily the best tool for dealing with the unique political threats to democracy created by platform scale. Straightforward state regulation, data portability, and privacy law have all been advanced as alternative tools to deal with platform scale.

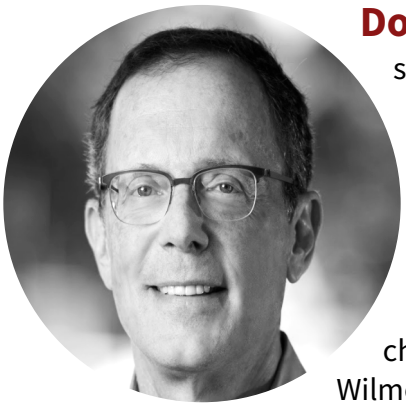
Middleware is another potential solution to this problem, and one that has not been adequately explored. It can take editorial power away from a small number of technology platforms and hand it not to a single government regulator, but to a diverse group of competitive firms that would allow users to tailor their online experiences. This approach would not prevent hate speech or conspiracy theories from circulating, but it would ensure that no single harmful idea will receive the amplification of a dominant information platform. It also ensures, in a way that aligns with the original intent of the First Amendment, that no one idea, whether disseminated by a platform or by those who manipulate them, will drown out all other speech. 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 over what they see. They—and not some invisible artificial intelligence program—would determine their ultimate online experience. We believe that this approach deserves further elaboration and testing, and should ultimately become the basis for new public policies.

Authors

Francis Fukuyama is the Olivier Nomellini Senior Fellow at Stanford University's Freeman Spogli Institute for International Studies (FSI), Mosbacher Director of FSI's Center on Democracy, Development, and the Rule of Law (CDDRL), and Director of Stanford's Masters in International Policy Program. He is also a professor (by courtesy) of Political Science. Dr. Fukuyama has written widely on issues in development and international politics. His 1992 book, *The End of History and the Last Man*, has appeared in over twenty foreign editions. His most recent book*, Identity: The Demand for Dignity and the Politics of Resentment*, was published in September 2018.

Barak Richman is the Katharine T. Bartlett Professor of Law and Business Administration at Duke University. His primary research interests include the economics of contracting, new institutional economics, antitrust, and health care policy. In 2006, he co-edited with Clark Havighurst a symposium volume of *Law and Contemporary Problems* entitled "Who Pays? Who Benefits? Distributional Issues in Health Care," and his book *Stateless Commerce* was published by Harvard University Press in 2017. During 2019-2020, he was a Visiting Scholar at the Stanford University School of Medicine and was a member of Stanford's Program on Democracy and the Internet's Working Group on Platform Scale.

Ashish Goel is a Professor of Management Science and Engineering and (by courtesy) Computer Science at Stanford University. He received his PhD in Computer Science from Stanford in 1999, and was an Assistant Professor of Computer Science at the University of Southern California from 1999 to 2002. His research interests lie in the design, analysis, and applications of algorithms.



Douglas Melamed practiced law for 43 years before spending the 2014-15 academic year at the Stanford Law School as the Herman Phleger Visiting Professor of Law. He was appointed Professor of the Practice of Law in 2015. From 2009 until 2014, Professor Melamed was Senior Vice President and General Counsel of Intel Corporation. Prior to joining Intel in 2009, he was a partner in the Washington, DC, office of WilmerHale, a global law firm in which he served as a chair of the Antitrust and Competition Practice Group. He joined WilmerHale's predecessor in 1971. From 1996 to 2001, Professor Melamed served in the US Department of Justice as Acting Assistant Attorney General in charge of the Antitrust Division and, before that, as Principal Deputy Assistant Attorney General. He is a Lifetime Member of the American Law Institute and a contributing editor of the *Antitrust Law Journal*.

Roberta Reiff Katz, lawyer and cultural anthropologist, is a Senior Research Scholar at the Center for Advanced Study in the Behavioral Sciences (CASBS) at Stanford University. At Stanford, she also served as Chief of Staff to the President and Associate VP for Strategic Planning. Ms. Katz was Special Advisor to the Assistant Attorney General for Antitrust, U.S. Department of Justice, in 2009-10. In prior years, Ms. Katz was CEO of the Technology Network (TechNet) and Senior VP and General Counsel of Netscape Communications Corporation and of McCaw Cellular Communications (now AT&T Wireless) and its subsidiary, LIN Broadcasting Corporation.

Marietje Schaake is the International Policy Director at Stanford University's Cyber Policy Center and International Policy Fellow at Stanford's Institute for Human-Centered Artificial Intelligence. She was named President of the Cyber Peace Institute. Between 2009 and 2019, Marietje served as a Member of European Parliament for the Dutch liberal democratic party where she focused on trade, foreign affairs, and technology policies. Marietje is affiliated with a number of nonprofits including the European Council on Foreign Relations and the Observer Research Foundation in India and writes a monthly column for the *Financial Times* and a bi-monthly column for the Dutch *NRC* newspaper.

[1] See Kate Conger and Davey Alba, "Twitter Refutes Inaccuracies in Trump's Tweets About Mail-In Voting," *The New York Times*, May 26, 2020, https://www.nytimes.com/2020/05/26/technology/twitter-trump-mail-in-ballots.html.
[2] Exec. Order No. 13925, 3 C.F.R. 34079-34083 (2020).
[3] See David Greene and Aaron Mackey, "Trump Executive Order Misreads Key Law Promoting Free Expression Online and Violates the First Amendment," Electronic Frontier Foundation, May 28, 2020, https://www.eff.org/deeplinks/2020/05/trump-executive-order-misreads-key-law-promoting-free-expression-online-and; Adam Serwer, "Trump's Warped Definition of Free Speech," *The Atlantic*, May 29, 2020, https://www.theatlantic.com/ideas/archive/2020/05/trumps-warped-definition-free-speech/612316/.
[4] Sheelah Kolhatkar, "The Growth of Sinclair's Conservative Media Empire," *The New Yorker*, October 15, 2018, https://www.newyorker.com/magazine/2018/10/22/the-growth-of-sinclairs-conservative-media-empire; Garrett Graff, "Fox News Is Now a Threat to National Security," *Wired*, December 11, 2019, https://www.wired.com/story/fox-news-is-now-a-threat-to-national-security/.
[5] Massachusetts. The Constitution of the State of Massachusetts, Adopted 1780: with the Amendments Annexed. Boston: Richardson and Lord, 1826.
[6] James Madison. Federalist No. 51: "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments." *New York Packet*, February 8, 1788.
[7] Stigler Committee on Digital Platforms, "Final Report," 2019, https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report; Jacques Crémer, Yves-Alexandre de Montjoye, and Heike Schweitzer, "Competition Policy For the Digital Era," 2019, https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en; Digital Competition Expert Panel, "Unlocking Digital Competition, Report of the Digital Competition Expert Panel," 2019, https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel.
[8] Erik Byrnjolfsson, Felix Eggers, and Avinash Gannamaneni, "Using Massive Online Choice Experiments to Measure Changes in Well-Being," *Proceedings of the National Academy of Sciences of the United States of America (PNAS)* 116, no. 15 (2019): 7250-7255.
[9] Byrnjolfsson, Eggers, and Gannamaneni, *supra* note 8.
[10] Gentzkow et al., "The Welfare Effects of Social Media," *American Economic Review* 110, no. 3 (2020): 629-676.
[11] Stigler Committee on Digital Platforms, *supra* note 9.
[12] Wikipedia, s.v. "List of mergers and acquisitions by Alphabet," last updated October 6, 2020, 16:10, https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet.
[13] See Zephyr Teachout and Lina Khan, "Market Structure and Political Law: A Taxonomy of Power," *Duke Journal of Constitutional Law & Public Policy* 9, no. 2 (2014): 37-74.
[14] Thomas Philippon, *The Great Reversal: How America Gave Up on Free Markets* (Cambridge, MA: Belknap Press 2019).
[15] See Article 7, European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02; Article 8, Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[16] Examples include Sermons v. Apple, No. 4:2019- cv-03796, N.D. Calif.; Frame-Wilson v. Amazon, No. 2:2020cv00424, W.D. Wash.; Mordy's Appliance Repair Service v. Amazon, No. 1:17-cv-05376, S.D.N.Y.; Ackers v. Google: No. 5:2019cv05537, N.D. Calif.
[17] See United States v. Apple, Inc. - 791 F.3d 290 (2d Cir. 2015); European Commission, "Antitrust: Commission accepts legally binding commitments from Penguin in e-books market," European Commission, July 25, 2013, https://ec.europa.eu/commission/presscorner/detail/en/IP_13_746.

[18] See European Commission, "Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine," European Commission, July 18, 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581.
[19] See European Commission, "Antitrust: Commission opens investigation into Apple's App Store rules," European Commission, June 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073.
[20] See Dana Mattioli, "Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products," *Wall Street Journal*, April 23, 2020, https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015.
[21] See Federal Trade Commission, "Statement of the Federal Trade Commission Regarding Google's Search Practices," Federal Trade Commission, January 3, 2013, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commission-regarding-googles-search-practices/130103brillgooglesearchstmt.pdf; European Commission, "Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service," European Commission, June 27, 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784.
[22] See Fiona Scott Morton and David Dinielli, "Roadmap for an Antitrust Case Against Facebook," Omidyar Network (2020); Dina Srinivasan, "Why Google Dominates Advertising Markets," *Stanford Technology Law Review* 24, forthcoming.
[23] See Williams Galston and Clara Hendrickson, "A policy at peace with itself: Antitrust remedies for our concentrated uncompetitive economy," Brookings Institution, January 5, 2018, https://www.brookings.edu/research/a-policy-at-peace-with-itself-antitrust-remedies-for-our-concentrated-uncompetitive-economy/; Senate Democrats, "A Better Deal," Senate Democratic Leadership, https://www.democrats.senate.gov/imo/media/doc/2017/07/A-Better-Deal-on-Competition-and-Costs-1.pdf; Amy Klobuchar, "Klobuchar Introduces Legislation to Modernize Antitrust Enforcement and Promote Competition," last modified February 1, 2019, https://www.klobuchar.senate.gov/public/index.cfm/2019/2/klobuchar-introduces-legislation-to-modernize-antitrust-enforcement-and-promote-competition.
[24] See Elizabeth Warren, "Here's How We Can Break Up Big Tech," Team Warren (blog), March 8, 2019, https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c; Bernie Sanders, "Corporate Accountability and Democracy," Bernie Sanders Official Website, 2019, https://berniesanders.com/issues/corporate-accountability-and-democracy/.
[25] See Open Markets Institute, "Open Markets Institute Calls on the FTC to Block All Facebook Acquisitions," Open Markets Institute, November 1, 2017, https://www.openmarketsinstitute.org/publications/open-markets-institute-calls-on-the-ftc-to-block-all-facebook-acquisitions/; Sergei Klebnikov, "Elizabeth Warren Reportedly Drafting Bill To Ban 'Mega-Mergers'," *Forbes*, December 5, 2019, https://www.forbes.com/sites/sergeiklebnikov/2019/12/05/elizabeth-warren-reportedly-drafting-bill-to-ban-mega-mergers/#32ae091266a4.
[26] Fiona Scott Morton and David Dinielli, "Roadmap for a Digital Advertising Monopolization Case Against Google" Omidyar Network (2020).
[27] Dina Srinivasan, "The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy," *Berkeley Business Law Journal* 16, no. 1 (2019): 39-101.
[28] See Robert Pitofsky, "Political Content of Antitrust," *University of Pennsylvania Law Review* 127, no. 4 (1979): 1051-1075; Robert Lande,"Consumer Choice as the Ultimate Goal of Antitrust," *University of Pittsburgh Law Review* 62, no. 3 (2001): 503-525.
[29] See, e.g., Reiter v. Sonotone Corp., 442 U.S. 330 (1979); Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209 (1993); Leegin Creative Leather Products, Inc. v. PSKS, Inc., 551 U.S. 877 (2007).
[30] See Douglas Melamed and Nicolas Petit, "The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets," *Review of Industrial Organization* 54 (2019): 741-774; Herbert Hovenkamp, *The Antitrust Enterprise* (Cambridge, MA: Harvard University Press, 2005).

[31] See F.M. Scherer and David Ross, *Industrial Market Structure and Economic Performance*, (Boston, MA: Houghton Mifflin Company, 1990).
[32] Luigi Zingales, "Towards a Political Theory of the Firm," *Journal of Economic Perspectives* 31, no. 3 (2017): 113-130.
[33] See Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York: Columbia Global Reports, 2018).
[34] See Maureen Ohlhausen and Alexander Okuliar, "Competition, Consumer Protection, and the Right [Approach] to Privacy," *Antitrust Law Journal* 80, no. 1 (2015): 121-156; Robert Lande, "The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern," FTC: Watch 714 (2008).
[35] See David McLaughlin and Scott Mortiz, "AT&T Probes White House Influence in Time Warner Case," Bloomberg, February 14, 2018, https://www.bloomberg.com/news/articles/2018-02-14/at-t-is-said-to-probe-white-house-influence-in-time-warner-case; Brian Fung and Tony Romm, "House Democrats Seek Records From Trump Over Reports of Possible Interference in AT&T-Time Warner Deal," *Washington Post*, March 7, 2019, https://www.washingtonpost.com/technology/2019/03/07/house-democrats-seek-records-trump-over-reports-possible-meddling-att-time-warner-deal/.
[36] Hiroko Tabuchi and Coral Davenport, "Justice Dept. Investigates California Emission Pact That Embarrassed Trump," *New York Times*, September 6, 2019, https://www.nytimes.com/2019/09/06/climate/automakers-california-emissions-antitrust.html.
[37] Department of Justice, "United States' Statement of Interest Concerning Qualcomm's Motion for Partial Stay of Injunction Pending Appeal" for Federal Trade Commission v. Qualcomm Incorporated 411 F. Supp. 3d 658 (N.D. Cal. 2019).
[38] Nicholas Fandos, "Justice Dept. Officials Outline Claims of Politicization Under Barr," *New York Times*, July 10, 2020, https://www.nytimes.com/2020/06/24/us/politics/justice-department-politicization.html.
[39] Article 20, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[40] See European Commission, "Can We Use Data for Another Purpose?" European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en.
[41] See Pranvera Kellezi, "Data Protection and Competition Law: Non-Compliance as Abuse of Dominant Position," *Sui-generis* (2019): 343-359.
[42] See Marco Botta, Klaus Wiedemann and Kimberly A. Houser, "The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey," *Antitrust Bulletin* 64, no. 3 (2019): 428-446.
[43] See Aysem Diker Vanberg and Mehmet Bilal Unver, "The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?" *European Journal of Law and Technology* 8, no. 1 (2017): 1-22.
[44] See Daniel L. Rubinfeld and Michael Gal, "Access Barriers to Big Data," *Arizona Law Review* 59, no. 339 (2017): 339-381.
[45] See Michal Gal and Oshrit Aviv, "The Competitive Effects of the GDPR," *Journal of Competition Law and Economics* (2020); Nicholas Martin et al., "How Data Protection Regulation Affects Startup Innovation," *Information Systems Frontiers* 21 (2019): 1307-1324.
[46] Lauren Jackson and Desiree Ibekwe, "Jack Dorsey on Twitter's Mistakes," *New York Times*, August 7, 2020, https://www.nytimes.com/2020/08/07/podcasts/the-daily/Jack-dorsey-twitter-trump.html.
[47] United States v. Microsoft (2001),# 253 F.3d 34 (D.C. Cir. 2001).
[48] Craig Timberg and Isaac Stanley-Becker, "QAnon Learns to Survive — and Even Thrive — After Silicon Valley's Crackdown," *Washington Post*, October 28, 2020, https://www.washingtonpost.com/technology/2020/10/28/qanon-crackdown-election/; Rachel Siegel, "8chan is back online, this time as 8kun," Washington Post, November 4, 2019, https://www.washingtonpost.com/technology/2019/11/04/chan-is-back-online-this-time-kun/.
[49] Stigler Committee on Digital Platforms, *supra* note 9.
[50] Digital Competition Expert Panel, *supra* note 9.

[51] Tom Wheeler, Phil Verveer, and Gene Kimmelman, "New Digital Realities; New Oversight Solutions," Shorenstein Center on Media, Politics and Public Policy, 2020, https://shorensteincenter.org/new-digital-realities-tom-wheeler-phil-verveer-gene-kimmelman/